

vSphere Single Host Management

Update 1

VMware vSphere 5.5

VMware ESXi 5.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001355-03

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2009–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

vSphere Single Host Management	7
Updated Information	9
1 Installing the vSphere Client	11
vSphere Client Hardware Requirements	11
vSphere Client Software Requirements	12
TCP and UDP Ports for the vSphere Client	12
Download the vSphere Client	13
Install the vSphere Client	13
Upgrade the vSphere Client	13
2 Using the vSphere Client	15
Start the vSphere Client and Log In	15
Stop the vSphere Client and Log Out	16
Getting Started Tabs	16
View Virtual Machine Console	17
Using Lists	17
Save vSphere Client Data	18
3 Configuring ESXi Hosts	19
Reboot or Shut Down an ESXi Host	19
Redirect the Direct Console to a Serial Port by Using the vSphere Client	19
Set the Scratch Partition from the vSphere Client	20
Configure Syslog on ESXi Hosts	20
Set the Host Image Profile Acceptance Level	21
4 Managing License Keys on ESXi Hosts	23
Access the ESXi License Key from the vSphere Client	23
Assign a License Key to an ESXi Host	23
View Which Features Are Licensed on a Host	24
Set an ESXi Host to Evaluation Mode	24
The License Key of an ESXi Host is Replaced	25
5 Managing Tasks	27
View Recent Tasks	27
Use Keywords to Filter the Tasks List	27
6 Securing ESXi Hosts	29
Allow or Deny Access to an ESXi Service or Management Agent	29
Add Allowed IP Addresses	30

- Set Service or Client Startup Options 30
- Disable Shell Access for Anonymous Users 30

7 ESXi Authentication and User Management 33

- Managing Users with the vSphere Client 33
- Password Requirements 35
- Assigning Permissions for ESXi 36
- Managing ESXi Roles 38
- Using Active Directory to Manage Users 40
- Using vSphere Authentication Proxy 41

8 Creating a Virtual Machine in the vSphere Client 43

- Start the Virtual Machine Creation Process in the vSphere Client 43
- Select a Configuration Option for the New Virtual Machine in the vSphere Client 44
- Enter a Name and Location for the Virtual Machine in the vSphere Client 45
- Select a Datastore in the vSphere Client 45
- Select a Virtual Machine Version in the vSphere Client 46
- Select an Operating System in the vSphere Client 46
- Select the Number of Virtual CPUs in the vSphere Client 47
- Configure Virtual Memory in the vSphere Client 47
- Configure Networks in the vSphere Client 48
- Select a SCSI Controller in the vSphere Client 49
- Selecting a Virtual Disk Type 49
- Complete Virtual Machine Creation in the vSphere Client 53

9 Deploying OVF Templates 55

- Deploy an OVF Template 55
- Browse VMware Virtual Appliance Marketplace 57
- Export an OVF Template 57

10 Configuring Virtual Machines in the vSphere Client 59

- Virtual Machine Hardware Versions 60
- Locate the Hardware Version of a Virtual Machine in the vSphere Client 61
- Change the Virtual Machine Name in the vSphere Client 61
- View the Virtual Machine Configuration File Location in the vSphere Client 62
- Edit Configuration File Parameters in the vSphere Client 62
- Change the Configured Guest Operating System in the vSphere Client 63
- Configure Virtual Machines to Automatically Upgrade VMware Tools 63
- Virtual CPU Configuration 64
- Virtual Memory Configuration 70
- Network Virtual Machine Configuration 74
- Parallel and Serial Port Configuration 75
- Virtual Disk Configuration 81
- Virtual MachineController Configuration 86
- Other Virtual Machine Device Configuration 89
- USB Configuration from an ESXi Host to a Virtual Machine 95
- USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client 100
- Add a Shared Smart Card Reader to Virtual Machines in the vSphere Client 106

Manage Power Management Settings for a Virtual Machine	106
Configure the Virtual Machine Power States	107
Delay the Boot Sequence in the vSphere Client	108
Enable Logging in the vSphere Client	109
Disable Acceleration in the vSphere Client	109
Configure Debugging and Statistics in the vSphere Client	109
11 Managing Virtual Machines	111
Edit Virtual Machine Startup and Shutdown Settings	111
Open a Console to a Virtual Machine	112
Remove Virtual Machines from a Host	112
Remove Virtual Machines from the Datastore	113
Return a Virtual Machine or Template to a Host	113
Using Snapshots To Manage Virtual Machines	113
12 Networking in the vSphere Client	123
View Networking Information in the vSphere Client	123
View Network Adapter Information in the vSphere Client	123
Setting Up Networking with vSphere Standard Switches	124
13 Managing Storage on a Single Host	129
Display Storage Devices for a Host in the vSphere Client	130
Display Storage Devices for an Adapter in the vSphere Client	130
View Storage Adapters Information in the vSphere Client	130
Review Datastore Information in the vSphere Client	130
Assign WWNs to Virtual Machines	130
Modify WWN Assignments	131
Set Up Networking for Software FCoE	132
Add Software FCoE Adapters	133
Disable Automatic Host Registration	133
Setting Up Independent Hardware iSCSI Adapters	134
Configuring Dependent Hardware iSCSI Adapters	135
Configuring Software iSCSI Adapters	137
Setting Up iSCSI Network	138
Using Jumbo Frames with iSCSI	143
Configuring Discovery Addresses for iSCSI Adapters	144
Configuring CHAP Parameters for iSCSI Adapters	146
Configure Advanced Parameters for iSCSI in the vSphere Client	149
Managing Storage Devices	149
Working with Datastores	151
14 Resource Management for Single Hosts	167
Configuring Resource Allocation Settings	167
Administering CPU Resources	168
Administering Memory Resources	171
Using NUMA Systems with ESXi	174
Advanced Attributes	175

15	Monitoring a Single Host with the vSphere Client	177
	Monitoring Host Health Status	177
	View Events	178
	View System Logs	179
	View Charts	179
	 Index	 181

vSphere Single Host Management

The *vSphere Single Host Management* documentation provides information on managing a single ESXi host through a direct connection from the vSphere Client. You can use these tasks to manage hosts that are not connected to vCenter Server, or to troubleshoot or manage hosts that have become disconnected from the vCenter System that normally managed them.

This documentation is intended primarily as a reference for tasks that you can perform when you connect directly to a host with the vSphere Client. For detailed information about vSphere networking, storage, security, virtual machine management, and other topics, see the appropriate vSphere documentation.

Intended Audience

This information is intended for anyone who wants to manage a single ESXi host by connecting directly to it with the vSphere Client. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information

This *vSphere Single Host Management* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Single Host Management* documentation.

Revision	Description
EN-001355-03	The information in “Configure the Virtual Machine Communication Interface in the vSphere Client,” on page 93 is updated to inform that the <code>vmci0.unrestricted</code> setting has no effect in ESXi 5.1 and later.
EN-001355-02	The table in “TCP and UDP Ports for the vSphere Client,” on page 12 was updated to clarify the direction of TCP and UDP traffic relative to the host.
EN-001355-01	■ The link to a VMware Knowledge Base article describing how to change the language used by the vSphere Client was updated in “Install the vSphere Client,” on page 13.
EN-001355-00	Initial release.

Installing the vSphere Client

Install the vSphere Client on a Windows system to connect to and manage single ESXi hosts.

To connect to and manage vCenter Server systems and the hosts connected to them, use the vSphere Web Client instead of the vSphere Client. Using the vSphere Web Client allows you to access a greater range of vSphere features and functionality than using the vSphere Client. For more information on installing the vSphere Web Client, see *vSphere Installation and Setup*.

This chapter includes the following topics:

- [“vSphere Client Hardware Requirements,”](#) on page 11
- [“vSphere Client Software Requirements,”](#) on page 12
- [“TCP and UDP Ports for the vSphere Client,”](#) on page 12
- [“Download the vSphere Client,”](#) on page 13
- [“Install the vSphere Client,”](#) on page 13
- [“Upgrade the vSphere Client,”](#) on page 13

vSphere Client Hardware Requirements

Make sure your system meets the hardware requirements for the vSphere Client.

vSphere Client Minimum Hardware Requirements and Recommendations

Table 1-1. vSphere Client Minimum Hardware Requirements and Recommendations

vSphere Client Hardware	Requirements and Recommendations
CPU	1 CPU
Processor	500MHz or faster Intel or AMD processor (1GHz recommended)
Memory	500MB (1GB recommended)

Table 1-1. vSphere Client Minimum Hardware Requirements and Recommendations (Continued)

vSphere Client Hardware	Requirements and Recommendations
Disk Storage	<p>1.5GB free disk space for a complete installation, which includes the following components:</p> <ul style="list-style-type: none"> ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# <p>Remove any previously installed versions of Microsoft Visual J# on the system where you are installing the vSphere Client.</p> <ul style="list-style-type: none"> ■ vSphere Client <p>If you do not have any of these components already installed, you must have 400MB free on the drive that has the %temp% directory.</p> <p>If you have all of the components already installed, 300MB of free space is required on the drive that has the %temp% directory, and 450MB is required for vSphere Client.</p>
Networking	Gigabit connection recommended

vSphere Client Software Requirements

Make sure that your operating system supports the vSphere Client.

For the most current, complete list of supported operating systems for the vSphere Client, see the VMware Compatibility Guide at <http://www.vmware.com/resources/compatibility>.

The vSphere Client requires the Microsoft .NET 3.5 SP1 Framework. If it is not installed on your system, the vSphere Client installer installs it. The .NET 3.5 SP1 installation might require Internet connectivity to download more files.

TCP and UDP Ports for the vSphere Client

ESXi hosts and other network components are accessed using predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports.

The table lists TCP and UDP ports, and the purpose and the type of each. Ports that are open by default at installation time are indicated by (Default).

Table 1-2. TCP and UDP Ports

Port	Purpose	Traffic Type
443 (Default)	<p>HTTPS access</p> <p>vSphere Client access to vCenter Server</p> <p>vSphere Client access to ESXi hosts</p> <p>vSphere Client access to vSphere Update Manager</p>	Incoming TCP to the ESXi host
902 (Default)	vSphere Client access to virtual machine consoles	Incoming TCP to the ESXi host, outgoing TCP from the ESXi host, outgoing UDP from the ESXi host
903	<p>Remote console traffic generated by user access to virtual machines on a specific host.</p> <p>vSphere Client access to virtual machine consoles</p> <p>MKS transactions (xinetd/vmware-authd-mks)</p>	Incoming TCP to the ESXi host

Download the vSphere Client

The vSphere Client is a Windows program that you can use to configure the host and to operate its virtual machines. You can download vSphere Client from any host.

Prerequisites

Verify that you have the URL of the host, which is the IP address or host name.

The system must have an Internet connection.

Procedure

- 1 From a Windows machine, open a Web browser.
- 2 Enter the URL or IP address for the vCenter Server or host.
For example, `http://exampleserver.example.com` or `http://xxx.xxx.xxx.xxx`.
- 3 Click **Download vSphere Client** under Getting Started.
- 4 Click **Save** to download the vSphere Client installer.

The vSphere Client installer is downloaded to the system.

What to do next

Install the vSphere Client.

Install the vSphere Client

The vSphere Client enables you to connect to an ESXi host.

When you use the vSphere Client, the vSphere Client appears in the language associated with the locale setting on the machine. You can alter this behavior with a command-line instruction. See KB 1016403: <http://kb.vmware.com/kb/1016403>.

Prerequisites

- Download the vSphere Client installer.
- Verify that you are a member of the Administrators group on the system.
- Verify that the system has an Internet connection.

Procedure

- 1 Double-click the `VMware-viclientbuild number.exe` file to run the vSphere Client installer.
- 2 Follow the prompts in the wizard to complete the installation.

What to do next

Connect to the host with the vSphere Client.

Upgrade the vSphere Client

Virtual machine users and vCenter Server administrators must use the vSphere Client 5.5 to connect to vCenter Server 5.5 or to connect directly to ESXi 5.5 hosts.

You can install the VI Client 2.5, the vSphere Client 4.x, and the vSphere Client 5.x on the same machine. After you upgrade vCenter Server, be sure to upgrade the vSphere Client to the same version to avoid compatibility problems that might interfere with the proper operation of the vSphere Client.

The vSphere Client upgrade operation requires no downtime. You do not need to power off virtual machines or clients.

Prerequisites

- Verify that you have the vCenter Server installer or the vSphere Client installer.
- Verify that you are a member of the Administrators group on the system.
- Verify that the system has an Internet connection.

Procedure

- 1 (Optional) Use **Add/Remove Programs** from the Windows Control Panel to remove any previous vCenter Server client.

You do not need to remove earlier versions of vCenter Server clients. These are useful if you need to connect to legacy hosts.

- 2 Run the vSphere Client installer.

- Start the vCenter Server installer. In the software installer directory, double-click the `autorun.exe` file and select **vSphere® Client™**.
- If you downloaded the vSphere Client, double-click the `VMware-viclient-build number.exe` file.

After you install the vSphere Client 5.5, you can connect to an ESXi host using the domain name or IP address of the host and the user name and password of a user on that machine.

What to do next

Use the vSphere Client to connect directly to an ESXi host using your user name and password.

If the vSphere Client displays security alerts and exceptions when you log in or perform some operations, such as opening performance charts or viewing the **Summary** tab, this might mean that your Internet Explorer (IE) security settings are set to High. If your IE security settings are set to High, enable the **Allow scripting of Internet Explorer web browser control** setting in IE.

Using the vSphere Client

The vSphere Client is the principal interface for administering vCenter Server and ESXi.

The vSphere Client user interface is configured based on the server to which it is connected:

- When the server is a vCenter Server system, the vSphere Client displays all the options available to the vSphere environment, according to the licensing configuration and the user permissions.
- When the server is an ESXi host, the vSphere Client displays only the options appropriate to single host management.

When you first log in to the vSphere Client, it displays a Home page with icons that you select to access vSphere Client functions. When you log out of the vSphere Client, the client application retains the view that was displayed when it closed, and returns you to that view when you next log in.

You perform many management tasks from the Inventory view, which consists of a single window containing a menu bar, a navigation bar, a toolbar, a status bar, a panel section, and pop-up menus.

This chapter includes the following topics:

- [“Start the vSphere Client and Log In,”](#) on page 15
- [“Stop the vSphere Client and Log Out,”](#) on page 16
- [“Getting Started Tabs,”](#) on page 16
- [“View Virtual Machine Console,”](#) on page 17
- [“Using Lists,”](#) on page 17
- [“Save vSphere Client Data,”](#) on page 18

Start the vSphere Client and Log In

The vSphere Client is a graphical user interface to vCenter Server and to hosts.

A login screen appears when you start the vSphere Client. After you log in, the client displays the objects and functionality appropriate to the server you are accessing and the permissions available to the user you logged in as.

Procedure

- 1 Log in to your Windows system.

If this is the first time you are starting the vSphere Client, log in as the administrator.

- If the managed host is not a domain controller, log in as either **local_host_name\user** or **user**, where **user** is a member of the local Administrators group.
- If the managed host is a domain controller, you must log in as **domain\userdomain\user**, where **domain** is the domain name for which the managed host is a controller and **user** is a member of that domain's Domain Administrators group. VMware does not recommend running on a domain controller.

- 2 Double-click a shortcut or select the vSphere Client from **Start > Programs > VMware > vSphere Client**.

- 3 Enter the server name, your user name, and your password.

If you are logging in to a vCenter Server system that is part of a Connected Group, logging in to that server connects you to all servers in that group.

NOTE Only previously entered server names appear in the **Server** drop-down menu.

- 4 Click **Login** to continue.

You are now connected to the host or vCenter Server system.

Stop the vSphere Client and Log Out

When you no longer need to view or alter the activities that the ESXi system is performing, log out of the vSphere Client.

NOTE Closing a vSphere Client session does not stop the host.

Procedure

- ◆ Click the close box (X), or select **File > Exit**.

The vSphere Client shuts down. The vSphere Client is logged out of the ESXi host. The host continues to run all its normal activities in the background.

Getting Started Tabs

In the case where ESXi is newly installed and no inventory objects have been added, the Getting Started tabs guide you through the steps of adding items to the inventory and setting up the virtual environment.

- [Disable Getting Started Tabs](#) on page 16

You can disable the Getting Started tabs if you do not want to display them.

- [Restore Getting Started Tabs](#) on page 17

If you turned off the display of the Getting Started tabs, you can restore the settings to display these tabs for all inventory objects.

Disable Getting Started Tabs

You can disable the Getting Started tabs if you do not want to display them.

You can disable the tabs in the following ways.

Procedure

- Click the **Close Tab** link to disable Getting Started tabs for the type of object selected.
- Change the vSphere Client settings to hide all Getting Started tabs.
 - a Select **Edit > Client Settings**.
 - b Select the **General** tab.
 - c Deselect the **Show Getting Started Tabs** check box and click **OK**.

Restore Getting Started Tabs

If you turned off the display of the Getting Started tabs, you can restore the settings to display these tabs for all inventory objects.

Procedure

- 1 Select **Edit > Client Settings**.
- 2 Click the **General** tab.
- 3 Select **Show Getting Started Tabs** and click **OK**.

View Virtual Machine Console

The console of a powered-on virtual machine is available through a connected server. All console connections to the virtual machine see the same information. The message line indicates if others are viewing the virtual machine.

Procedure

- 1 Select a powered-on virtual machine.
- 2 In the Information panel, click the **Console** tab.
- 3 (Optional) Click the pop-out icon in the navigation bar to show the virtual machine console in a separate window.
- 4 (Optional) Press Ctrl+Alt+Enter to enter or exit full screen mode.

Using Lists

Many vSphere Client inventory tabs display lists of information.

For example, the **Virtual Machines** tab displays a list of all the virtual machines associated with a host or a cluster. Sort any list in the vSphere Client by clicking the column label heading. A triangle in the column head shows the sort order as ascending or descending.

You can also filter a list, sorting and including only selected items. A filter is sorted by a keyword. Select the columns to include in the search for the keyword.

Filter a List View

You can filter a list if it is too long, or if you are looking for specific items in the list (alarms that begin with the word "datastore," for example). You can show and hide the filter field by using the **Filtering** option in the **View** menu.

The list is updated based on whether filtering is on or off. For example, if you are in the **Virtual Machines** tab, you have filtered the list and the filtered text is "powered on." You see a list of virtual machines whose state is set to powered on. If the state of any virtual machine changes, the virtual machine is removed from the list. Virtual machines that are added to the list are also filtered.

Procedure

- 1 On any inventory panel that displays a list, click the arrow next to the filter box at the top right of the pane.
- 2 Select the attributes on which to filter.
- 3 Enter search criteria into the filter field.

The search automatically starts after a pause of more than one second. Neither boolean expressions nor special characters are supported. Filtering is not case-sensitive.

- 4 (Optional) Click **Clear** to clear the filter field.

Export a List

You can export a list to a file.

Procedure

- 1 Select the list to export.
- 2 Select **File > Export > Export List**.
- 3 Type a filename and select a file type.
- 4 Click **Save**.

Save vSphere Client Data

The vSphere Client user interface is similar to a browser. Most user actions are persistent in ESXi data that appears. You typically do not have to save the data.

Procedure

- ◆ You can save the client data by either printing a copy of the window or exporting the server data.

Option	Description
Copy the window	Use the Microsoft Windows Print Screen option to print a copy of the vSphere Client window.
Export server data	Select File > Export and select a format in which to save the data. Open the data in an appropriate application and print from that application.

Configuring ESXi Hosts

When you connect directly to an ESXi host with the vSphere Client, you can perform a variety of configuration tasks such as setting the scratch partition, redirecting the direct console, and configuring syslog.

This chapter includes the following topics:

- [“Reboot or Shut Down an ESXi Host,”](#) on page 19
- [“Redirect the Direct Console to a Serial Port by Using the vSphere Client,”](#) on page 19
- [“Set the Scratch Partition from the vSphere Client,”](#) on page 20
- [“Configure Syslog on ESXi Hosts,”](#) on page 20
- [“Set the Host Image Profile Acceptance Level,”](#) on page 21

Reboot or Shut Down an ESXi Host

You can power off or restart (reboot) any ESXi host using the vSphere Client. Powering off a managed host disconnects it from vCenter Server, but does not remove it from the inventory.

Procedure

- 1 Shut down all virtual machines running on the ESXi host.
- 2 Select the ESXi host you want to shut down.
- 3 From the main or right-click menu, select **Reboot** or **Shut Down**.
 - If you select **Reboot**, the ESXi host shuts down and reboots.
 - If you select **Shut Down**, the ESXi host shuts down. You must manually power the system back on.
- 4 Provide a reason for the shut down.

This information is added to the log.

Redirect the Direct Console to a Serial Port by Using the vSphere Client

You can redirect the direct console to either of the serial ports com1 or com2. When you use the vSphere Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

Prerequisites

- Verify that you can access the host from the vSphere Client.

- Verify that the serial port is not already be in use for serial logging and debugging, or for ESX Shell (tty1Port).

Procedure

- 1 From the vSphere Client, connect to the vCenter Server and select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, click **Advanced Settings**.
- 4 In the left pane, expand the **VMkernel** listing and select **Boot**.
- 5 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.
- 6 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: **com1** or **com2**.
- 7 Click **OK**.
- 8 Reboot the host.

You can now manage the ESXi host remotely from a console that is connected to the serial port.

Set the Scratch Partition from the vSphere Client

If a scratch partition is not set up, you might want to configure one, especially if low memory is a concern. When a scratch partition is not present, vm-support output is stored in a ramdisk.

Prerequisites

The directory to use for the scratch partition must exist on the host.

Procedure

- 1 Use the vSphere Client to connect to the host.
- 2 Select the host in the Inventory.
- 3 In the **Configuration** tab, select **Software**.
- 4 Select **Advanced Settings**.
- 5 Select **ScratchConfig**.
The field **ScratchConfig.CurrentScratchLocation** shows the current location of the scratch partition.
- 6 In the field **ScratchConfig.ConfiguredScratchLocation**, enter a directory path that is unique for this host.
- 7 Reboot the host for the changes to take effect.

Configure Syslog on ESXi Hosts

All ESXi hosts run a syslog service (vmsyslogd), which logs messages from the VMkernel and other system components to log files.

You can use the vSphere Client or the `esxcli system syslog vCLI` command to configure the syslog service.

For more information about using vCLI commands, see *Getting Started with vSphere Command-Line Interfaces*.

Procedure

- 1 In the vSphere Client inventory, select the host.
- 2 Click the **Configuration** tab.

- 3 In the Software panel, click **Advanced Settings**.
- 4 Select **Syslog** in the tree control.
- 5 To set up logging globally, click **global** and make changes to the fields on the right.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the <code>/scratch</code> directory on the local file system is persistent across reboots. The directory should be specified as <code>[datastorename] path_to_file</code> where the path is relative to the root of the volume backing the datastore. For example, the path <code>[storage1] /systemlogs</code> maps to the path <code>/vmfs/volumes/storage1/systemlogs</code> .
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by Syslog.global.LogDir . A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, <code>ssl://hostName1:514</code> . UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

- 6 (Optional) To overwrite the default log size and log rotation for any of the logs.
 - a Click **loggers**.
 - b Click the name of the log you that want to customize and enter the number of rotations and log size you want.
- 7 Click **OK**.

Changes to the syslog options take effect immediately.

Set the Host Image Profile Acceptance Level

The Host Image Profile acceptance level determines which vSphere installation bundles (VIBs) are accepted for installation.

VIB signatures are checked and accepted for installation based on a combination of the VIB acceptance level and the host image profile acceptance level. VIBs are tagged with an acceptance level that depends on their signature status.

Prerequisites

Required privileges: **Host.Configuration.SecurityProfile** and **Host.Configuration.Firewall**

Procedure

- 1 Use the vSphere Client to access the host in one of the following ways.
 - Connect to the host directly.
 - Connect to vCenter Server, and select the host in the inventory.
- 2 Click the **Configuration** tab.

- 3 Under Software, click **Security Profile**.
- 4 Under Host Image Profile Acceptance Level, click **Edit**.
- 5 Select the acceptance level and click **OK**.

Table 3-1. Host Image Profile Acceptance Levels

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMwareCertified	VMwareCertified
VMwareAccepted	VMwareCertified, VMwareAccepted
PartnerSupported	VMwareCertified, VMwareAccepted, PartnerSupported
CommunitySupported	VMwareCertified, VMwareAccepted, PartnerSupported, CommunitySupported

Managing License Keys on ESXi Hosts

4

When you connect the vSphere Client directly to an ESXi host, you can view and assign license keys, see which features are licensed on the host, and put the host in evaluation mode.

This chapter includes the following topics:

- [“Access the ESXi License Key from the vSphere Client,”](#) on page 23
- [“Assign a License Key to an ESXi Host,”](#) on page 23
- [“View Which Features Are Licensed on a Host,”](#) on page 24
- [“Set an ESXi Host to Evaluation Mode,”](#) on page 24
- [“The License Key of an ESXi Host is Replaced,”](#) on page 25

Access the ESXi License Key from the vSphere Client

If you are not local to the host and cannot access the direct console, use the vSphere Client to access the ESXi license key.

Procedure

- 1 From the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab and click **Licensed Features**.

The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Assign a License Key to an ESXi Host

You can assign a license key to an ESXi host from the Licensing page in the vSphere Client.

If the vSphere Client is connected directly to the host, on the host **Configuration** tab click **Licensed Features** > **Edit** to change the license key.

Prerequisites

Verify that you have the **Global.Licenses** privilege.

Procedure

- 1 Select the host in the inventory and click the **Configuration** tab.
- 2 Click **Licensed Features** and click **Edit**.

- 3 Assign a license key.
 - Select **Assign an existing license key to this host** and select a license key from the Product list.
 - Select **Assign a new license key to this host**, click **Enter Key**, and specify a license key and an optional label for the license key.
- 4 Click **OK**.

View Which Features Are Licensed on a Host

You can view which features a host is licensed to use.

If you try to configure features that are not included in the host license, the vSphere Client displays an error message.

Procedure

- 1 From the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, click **Licensed Features**.

The list appears of features that you can configure on the host.

Set an ESXi Host to Evaluation Mode

If you have assigned a license key to an ESXi host, you can switch to evaluation mode to explore the full set of features that are available for the host..

Procedure

- 1 From the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, click **Licensed Features**.
- 4 Click **Edit** next to ESX Server License Type.
- 5 Click **Product Evaluation**.
- 6 Click **OK** to save your changes.

The host is in evaluation mode and you can explore the entire set of features for ESXi. If you have already used the host in evaluation mode, the time that remains in the evaluation period is decreased by the time already used. For example, suppose you have used the host in evaluation mode for 20 days and then assigned a vSphere Standard license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features that are available for the host for the remaining evaluation period of 40 days. You can track the remaining days from the evaluation period of a host in the host's page in the vSphere Client.

NOTE After the evaluation period of the host expires, you receive a warning message, and the host cannot be connected to a vCenter Server system. All powered-on virtual machines continue to work, but you cannot power on any new virtual machines. You cannot change the current configuration of the features that are already in use. You cannot use the features that remained unused while the host was in evaluation mode.

The License Key of an ESXi Host is Replaced

The license key that you assigned through a direct connection with the vSphere Client to an ESXi host changes.

Problem

You use the vSphere Client to connect directly to an ESXi host. You use the **Configuration > Licensed Features > Edit** operation to assign a license key to the host. Later, a different license key replaces the license key you assigned to the host.

Cause

If a vCenter Server system manages an ESXi host, changes made to the host license through direct connection to the host do not persist, because the license key assigned through vCenter Server overwrites the changes.

If you use the **Configuration > Licensed Features > Edit** operation, any license assignment operation that you perform in vCenter Server overrides the host license configuration.

Solution

If you use vCenter Server to manage the host through vCenter Server, use either the **Home > Administration > Licensing** interface or the Add Host operation to configure host licensing.

Managing Tasks

Tasks represent system activities that do not complete immediately, such as migrating a virtual machine. They are initiated by high-level activities that you perform with the vSphere Client in real time and activities that you schedule to occur at a later time or on a recurring basis.

For example, powering off a virtual machine is a task. You can perform this task manually every evening, or you can set up a scheduled task to power off the virtual machine every evening for you.

NOTE The functionality available in the vSphere Client depends on whether the vSphere Client is connected to a vCenter Server system or an ESXi host. Unless indicated, the process, task, or description applies to both kinds of vSphere Client connections. When the vSphere Client is connected to an ESXi host, the **Tasks** option is not available; however, you can view recent tasks in the **Status Bar** at the bottom of the vSphere Client.

This chapter includes the following topics:

- [“View Recent Tasks,”](#) on page 27
- [“Use Keywords to Filter the Tasks List,”](#) on page 27

View Recent Tasks

You view recent tasks for an ESXi host in the vSphere Client **Recent Tasks** pane.

Procedure

- 1 Display the Inventory panel.
- 2 Select the object.
- 3 If necessary, select **View > Status** to display the status bar at the bottom of the vSphere Client.

The list of completed tasks appears in the **Recent Tasks** pane of the **Status Bar**.

Use Keywords to Filter the Tasks List

You can filter the tasks list based on any task attribute, including task name, target, status, initiator, change history, and time. Filtering is inclusive, not exclusive. If the keyword is found in any of the selected columns, the task is included in the filtered list.

Procedure

- 1 Select the object in the inventory.
- 2 If the **Name, Target or Status contains** search field is not displayed above the Recent Tasks pane, select **View > Filtering**.

- 3 Click the search field arrow and select the attributes to include in the search.
- 4 Type a keyword into the box and press Enter.

Securing ESXi Hosts

Restricting access to the services and ports on an ESXi host is critical to protecting against unauthorized intrusion in your vSphere environment.

If a host is compromised, the virtual machines on that host are now threatened to be compromised as well. Restrict access to services and ports, an ESXi host is protected with a firewall. Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment.

This chapter includes the following topics:

- [“Allow or Deny Access to an ESXi Service or Management Agent,”](#) on page 29
- [“Add Allowed IP Addresses,”](#) on page 30
- [“Set Service or Client Startup Options,”](#) on page 30
- [“Disable Shell Access for Anonymous Users,”](#) on page 30

Allow or Deny Access to an ESXi Service or Management Agent

You can configure firewall properties to allow or deny access for a service or management agent.

You add information about allowed services and management agents to the host configuration file. You can enable or disable these services and agents using the vSphere Client or at the command line.

NOTE If different services have overlapping port rules, enabling one service might implicitly enable overlapping services. To minimize the effects of this behavior, you can specify which IP addresses are allowed to access each service on the host.

Procedure

- 1 Select the host in the inventory panel.
- 2 Click the **Configuration** tab and click **Security Profile**.

The vSphere Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.
- 3 In the Firewall section, click **Properties**.

The Firewall Properties dialog box lists all the rule sets that you can configure for the host.
- 4 Select the rule sets to enable, or deselect the rule sets to disable.

The Incoming Ports and Outgoing Ports columns indicate the ports that the vSphere Client opens for the service. The Protocol column indicates the protocol that the service uses. The Daemon column indicates the status of daemons associated with the service.
- 5 Click **OK**.

Add Allowed IP Addresses

You can specify which networks are allowed to connect to each service that is running on the host.

You can use the vSphere Client or the command line to update the Allowed IP list for a service. By default, all IP addresses are allowed.

Procedure

- 1 Select the host in the inventory panel.
- 2 Click the **Configuration** tab and click **Security Profile**.
- 3 In the Firewall section, click **Properties**.
- 4 Select a service in the list and click **Firewall**.
- 5 Select **Only allow connections from the following networks** and enter the IP addresses of networks that are allowed to connect to the host.

You can enter IP addresses in the following formats: 192.168.0.0/24, 192.168.1.2, 2001::1/64, or fd3e:29a6:0a81:e478::/64.

- 6 Click **OK**.

Set Service or Client Startup Options

By default, daemon processes start when any of their ports are opened and stop when all of their ports are closed. You can change this startup policy for the selected service or client.

Procedure

- 1 Log in to a vCenter Server system using the vSphere Web Client.
- 2 Select the host in the inventory panel.
- 3 Click the **Configuration** tab and click **Security Profile**.
- 4 In the Firewall section, click **Properties**.

The Firewall Properties dialog box lists all the services and management agents you can configure for the host.

- 5 Select the service or management agent to configure and click **Options**.

The Startup Policy dialog box determines when the service starts. This dialog box also provides information about the current state of the service and provides an interface for manually starting, stopping, or restarting the service.

- 6 Select a policy from the **Startup Policy** list.
- 7 Click **OK**.

Disable Shell Access for Anonymous Users

To prevent anonymous users such as root from accessing the host with the Direct Console User Interface (DCUI) or ESXi Shell, remove the user's administrator privileges on the root folder of the host. This applies to both local users and Active Directory users and groups.

Procedure

- 1 Log in to ESXi using the vSphere Client.
- 2 Click the **Local Users & Groups** tab and click **Users**.

- 3 Right-click the anonymous user (for example, root) in the Users table and click **Properties**.
- 4 Select an access role from the drop-down list.
- 5 Click **OK**.

What to do next

By default, available roles are No access, Administrator, and Read-only. You can create new roles to apply to the user, as described in [“Managing ESXi Roles,”](#) on page 38.

ESXi Authentication and User Management

7

ESXi handles user authentication and supports user permissions.

When you connect directly to an ESXi host with the vSphere Client, you can create users and groups that are local to that ESXi host. You can also assign permissions to these users and groups.

vCenter Server is not aware of users that are local to ESXi, and ESXi is not aware of vCenter Server users. For more information on managing users for ESXi hosts managed by vCenter Server, see the *vSphere Security* documentation.

This chapter includes the following topics:

- [“Managing Users with the vSphere Client,”](#) on page 33
- [“Password Requirements,”](#) on page 35
- [“Assigning Permissions for ESXi,”](#) on page 36
- [“Managing ESXi Roles,”](#) on page 38
- [“Using Active Directory to Manage Users,”](#) on page 40
- [“Using vSphere Authentication Proxy,”](#) on page 41

Managing Users with the vSphere Client

Manage users to control who is authorized to log in to ESXi.

In vSphere 5.1 and later, ESXi user management has the following caveats.

- The users created when you connect directly to an ESXi host are not the same as the vCenter Server users. When the host is managed by vCenter Server, vCenter Server ignores users created directly on the host.
- You cannot create ESXi users with the vSphere Web Client. You must log directly into the host with the vSphere Client to create ESXi users.
- ESXi 5.1 and later does not support local groups. However, Active Directory groups are supported.

To prevent anonymous users such as root from accessing the host with the Direct Console User Interface (DCUI) or ESXi Shell, remove the user's administrator privileges on the root folder of the host. This applies to both local users and Active Directory users and groups.

Add a Local ESXi User

Adding a user to the users table updates the internal user list that the host maintains.

Prerequisites

Review the password requirements described in [“Password Requirements,”](#) on page 35.

Procedure

- 1 Log in to ESXi using the vSphere Client.

You cannot create ESXi users with the vSphere Web Client. You must directly log into the host with the vSphere Client to create ESXi users.

- 2 Click the **Local Users & Groups** tab and click **Users**.
- 3 Right-click anywhere in the Users table and click **Add**.
- 4 Enter a login, a user name, and a password.

NOTE Do not create a user named **ALL**. Privileges associated with the name **ALL** might not be available to all users in some situations. For example, if a user named **ALL** has Administrator privileges, a user with **ReadOnly** privileges might be able to log in to the host remotely. This is not the intended behavior.

- Specifying the user name and UID are optional.
- Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error.
- ESXi 5.1 does not support local groups.

- 5 Click **OK**.

Modify the Settings for a User on the Host

You can change the user ID, user name, and password for a user.

Prerequisites

Review the password requirements as described in [“Password Requirements,”](#) on page 35.

Procedure

- 1 Log in to ESXi using the vSphere Client.

You cannot create ESXi users with the vSphere Web Client. You must log directly into the host with the vSphere Client to create ESXi users.

- 2 Click the **Local Users & Groups** tab and click **Users**.
- 3 Right-click the user and click **Edit** to open the Edit User dialog box.
- 4 Enter a login, a user name, and a password.

NOTE Do not create a user named **ALL**. Privileges associated with the name **ALL** might not be available to all users in some situations. For example, if a user named **ALL** has Administrator privileges, a user with **ReadOnly** privileges might be able to log in to the host remotely. This is not the intended behavior.

- Specifying the user name and UID are optional.
- Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error.
- ESXi 5.1 does not support local groups.

- 5 Click **OK**.

Remove a Local ESXi User from a Host

You can remove a local ESXi user from the host.



CAUTION Do not remove or rename the root user.

If you remove a user from the host, they lose permissions to all objects on the host and cannot log in again.

NOTE Users who are logged in and are removed from the domain keep their host permissions until you restart the host.

Procedure

- 1 Log in to ESXi using the vSphere Client.
- 2 Click the **Local Users & Groups** tab and click **Users**.
- 3 Right-click the user to remove and select **Remove**.

Do not remove the root user for any reason.

Sort, Export, and View Local ESXi Users

You can view, sort, and export lists of a host's local users to a file that is in HTML, XML, Microsoft Excel, or CSV format.

Procedure

- 1 Log in to ESXi using the vSphere Client.
- 2 Click the **Local Users & Groups** tab and click **Users**.
- 3 Determine how to sort the table, and hide or show columns according to the information you want to see in the exported file.
 - To sort the table by any of the columns, click the column heading.
 - To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.
 - To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.
- 4 Right-click anywhere in the table and click **Export List** to open the Save As dialog box.
- 5 Select a path and enter a filename.
- 6 Select the file type and click **OK**.

Password Requirements

By default, ESXi enforces requirements for user passwords.

When you create a password, include a mix of characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters such as an underscore or dash.

Your user password must meet the following length requirements.

- Passwords containing characters from one or two character classes must be at least eight characters long.
- Passwords containing characters from three character classes must be at least seven characters long.

- Passwords containing characters from all four character classes must be at least six characters long.

The password cannot contain the words root, admin, or administrator in any form.

NOTE An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

You can also use a passphrase, which is a phrase consisting of at least three words, each of which is 8 to 40 characters long.

Example: Creating Acceptable Passwords

The following password candidates meet the requirements of ESXi.

- xQaTEhbU: Contains eight characters from two character classes.
- xQaT3pb: Contains seven characters from three character classes.
- xQaT3#: Contains six characters from four character classes.

The following password candidates do not meet the requirements of ESXi.

- Xqat3hb: Begins with an uppercase character, reducing the effective number of character classes to two. Eight characters are required when you use only two character classes.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. Eight characters are required when you use only two character classes.

Assigning Permissions for ESXi

For ESXi, permissions are defined as access roles that consist of a user and the user's assigned role for an object such as a virtual machine or ESXi host. Permissions grant users the right to perform the activities specified by the role on the object to which the role is assigned.

For example, to configure memory for the host, a user must be granted a role that includes the **Host.Configuration.Memory Configuration** privilege. By assigning different roles to users for different objects, you can control the tasks that users can perform in your vSphere environment.

When connecting directly to a host with the vSphere Client, the root and vpxuser user accounts have the same access rights as any user assigned the Administrator role on all objects.

All other users initially have no permissions on any objects, which means they cannot view these objects or perform operations on them. A user with Administrator privileges must assign permissions to these users to allow them to perform tasks.

Many tasks require permissions on more than one object. These rules can help you determine where you must assign permissions to allow particular operations:

- Any operation that consumes storage space, such as creating a virtual disk or taking a snapshot, requires the **Datastore.Allocate Space** privilege on the target datastore, as well as the privilege to perform the operation itself.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege.

The list of privileges is the same for both ESXi and vCenter Server.

You can create roles and set permissions through a direct connection to the ESXi host.

Permission Validation

vCenter Server and ESXi hosts that use Active Directory regularly validate users and groups against the Windows Active Directory domain. Validation occurs whenever the host system starts and at regular intervals specified in the vCenter Server settings.

For example, if user Smith was assigned permissions and in the domain the user's name was changed to Smith2, the host concludes that Smith no longer exists and removes permissions for that user when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions are removed when the next validation occurs. If a new user Smith is added to the domain before the next validation occurs, the new user Smith receives all the permissions the old user Smith was assigned.

Replace the Authentication Proxy Certificate for the ESXi Host

You can import a certificate from a trusted certificate authority from the vSphere Web Client

Prerequisites

- Upload the authentication proxy certificate file to the ESXi host.

Procedure

- 1 In the vSphere Web Client, select the ESXi host.
- 2 In the **Settings** tab, select **Authentication Services** in the **System** area.
- 3 Click **Import Certificate**.
- 4 Enter the SSL certificate path and the vSphere Authentication Proxy server.

Change Permissions

After a user and role pair is set for an inventory object, you can change the role paired with the user or change the setting of the **Propagate** check box. You can also remove the permission setting.

Procedure

- 1 From the vSphere Client, select an object in the inventory.
- 2 Click the **Permissions** tab.
- 3 Right-click the line item to select the user and role pair.
- 4 Select **Properties**.
- 5 Select a role for the user or group from the drop-down menu.
- 6 To propagate the privileges to the children of the assigned inventory object, click the **Propagate** check box and click **OK**.

Remove Permissions

Removing a permission for a user or group does not remove the user or group from the list of those available. It also does not remove the role from the list of available items. It removes the user or group and role pair from the selected inventory object.

Procedure

- 1 From the vSphere Client, click the **Inventory** button.
- 2 Expand the inventory as needed and click the appropriate object.

- 3 Click the **Permissions** tab.
- 4 Click the appropriate line item to select the user or group and role pair.
- 5 Select **Inventory > Permissions > Delete**.

Managing ESXi Roles

ESXi grants access to objects only to users who are assigned permissions for the object. When you assign a user permissions for the object, you do so by pairing the user with a role. A role is a predefined set of privileges.

ESXi hosts provide three default roles, and you cannot change the privileges associated with these roles. Each subsequent default role includes the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role. Roles you create yourself do not inherit privileges from any of the default roles.

You can create custom roles by using the role-editing facilities in the vSphere Client to create privilege sets that match your user needs. If you use the vSphere Client connected to vCenter Server to manage ESXi hosts, you have additional roles to choose from in vCenter Server. Also, the roles you create directly on a host are not accessible within vCenter Server. You can work with these roles only if you log in to the host directly from the vSphere Client.

Note When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: System.Anonymous, System.View, and System.Read.

If you manage ESXi hosts through vCenter Server, maintaining custom roles in the host and vCenter Server can result in confusion and misuse. In this type of configuration, maintain custom roles only in vCenter Server.

You can create host roles and set permissions through a direct connection to the ESXi host with the vSphere Client.

Create a Role

VMware recommends that you create roles to suit the access control needs of your environment.

Prerequisites

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

Procedure

- 1 On the vSphere Client Home page, click **Roles**.
- 2 Right-click the **Roles** tab information panel and click **Add**.
- 3 Type a name for the new role.
- 4 Select privileges for the role and click **OK**.

Clone a Role

You can make a copy of an existing role, rename it, and later edit it. When you make a copy, the new role is not applied to any users or groups and objects. You must assign the role to users or groups and objects.

Prerequisites

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

Procedure

- 1 On the vSphere Client Home page, click **Roles**.

- 2 To select the role to duplicate, click the object in the list of **Roles**.
- 3 To clone the selected role, select **Administration > Role > Clone**.

A duplicate of the role is added to the list of roles. The name is *Copy of rolename*.

Edit a Role

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group assigned the edited role.

Prerequisites

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

Procedure

- 1 On the vSphere Client Home page, click **Roles**.
- 2 Right-click the role to edit and select **Edit Role**.
- 3 Select privileges for the role and click **OK**.

Rename a Role

When you rename a role, no changes occur to that role's assignments.

Prerequisites

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

Procedure

- 1 On the vSphere Client Home page, click **Roles**.
- 2 Click the object in the list of roles that you want rename.
- 3 Select **Administration > Role > Rename**.
- 4 Type the new name.

Remove a Role

When you remove a role that is not assigned to any users or groups, the definition is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.



CAUTION You must understand how users will be affected before removing all assignments or replacing them. Users who have no permissions granted to them cannot log in.

Prerequisites

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

Procedure

- 1 On the vSphere Client Home page, click **Roles**.
- 2 Click the object you want to remove in the list of roles.
- 3 Select **Administration > Role > Remove**.

- 4 Click **OK**.

The role is removed from the list.

If the role is assigned to a user or group, a warning message appears.

- 5 Select a reassignment option and click **OK**.

Option	Description
Remove Role Assignments	Removes configured user or group and role pairings on the server. If a user or group does not have other permissions assigned, they lose all privileges.
Reassign affected users to	Reassigns any configured user or group and role pairings to the selected new role.

Using Active Directory to Manage Users

You can configure ESXi to use a directory service such as Active Directory to manage users.

Creating local user accounts on each host presents challenges with having to synchronize account names and passwords across multiple hosts. Join ESXi hosts to an Active Directory domain to eliminate the need to create and maintain local user accounts. Using Active Directory for user authentication simplifies the ESXi host configuration and reduces the risk for configuration issues that could lead to unauthorized access.

When you use Active Directory, users supply their Active Directory credentials and the domain name of the Active Directory server when adding a host to a domain.

Configure a Host to Use Active Directory

You can configure the host to use a directory service such as Active Directory to manage users and groups.

Prerequisites

- Verify that you have an Active Directory domain. See your directory server documentation.
- Verify that the host name of ESXi is fully qualified with the domain name of the Active Directory forest.
fully qualified domain name = host_name.domain_name

Procedure

- 1 Synchronize the time between ESXi and the directory service system using NTP.
ESXi supports synchronizing time with an external NTPv3 or NTPv4 server that is compliant with RFC 5905 and RFC 1305. The Microsoft Windows W32Time service does not meet these requirements when running with default settings. See the *vSphere Security* documentation or the VMware Knowledge Base for information about how to synchronize ESXi time with a Microsoft Domain Controller.
- 2 Ensure that the DNS servers you configured for the host can resolve the host names for the Active Directory controllers.
 - a In the vSphere Client, select the host in the inventory.
 - b Click the **Configuration** tab and click **DNS and Routing**.
 - c Click the **Properties** link at the top right of the panel.
 - d In the DNS and Routing Configuration dialog box, verify that the host name and DNS server information for the host are correct.

What to do next

Use the vSphere Client to join a directory service domain.

Add a Host to a Directory Service Domain

To use a directory service, you must join the host to the directory service domain.

You can enter the domain name in one of two ways:

- **name.tld** (for example, **domain.com**): The account is created under the default container.
- **name.tld/container/path** (for example, **domain.com/OU1/OU2**): The account is created under a particular organizational unit (OU).

To use the vSphere Authentication Proxy service (CAM service), see the *vSphere Security* documentation.

Prerequisites

Verify that the vSphere Client is connected to the host.

Procedure

- 1 Select a host in the vSphere Client inventory, and click the **Configuration** tab.
- 2 Click **Properties**.
- 3 In the Directory Services Configuration dialog box, select the directory service from the drop-down menu.
- 4 Enter a domain.
Use the form **name.tld** or **name.tld/container/path**.
- 5 Click **Join Domain**.
- 6 Enter the user name and password of a directory service user who has permissions to join the host to the domain, and click **OK**.
- 7 Click **OK** to close the Directory Services Configuration dialog box.

View Directory Service Settings

You can view the type of directory server, if any, the host uses to authenticate users and the directory server settings.

Procedure

- 1 Select a host in the vSphere Client inventory, and click the **Configuration** tab.
- 2 Under Software, select **Authentication Services**.

The Authentication Services Settings page displays the directory service and domain settings.

Using vSphere Authentication Proxy

When you use the vSphere Authentication Proxy, you do not need to transmit Active Directory credentials to the host. Users supply the domain name of the Active Directory server and the IP address of the authentication proxy server when they add a host to a domain.

Use vSphere Authentication Proxy to Add a Host to a Domain

When you join a host to a directory service domain, you can use the vSphere Authentication Proxy server for authentication instead of transmitting user-supplied Active Directory credentials.

You can enter the domain name in one of two ways:

- **name.tld** (for example, **domain.com**): The account is created under the default container.

- **name.tld/container/path** (for example, **domain.com/OU1/OU2**): The account is created under a particular organizational unit (OU).

Prerequisites

- Verify that the vSphere Client is connected to the host.
- If ESXi is configured with a DHCP address, set up the DHCP range as described in the *vSphere Security* documentation..
- If ESXi is configured with a static IP address, verify that its associated profile is configured to use the vSphere Authentication Proxy service to join a domain so that the authentication proxy server can trust the ESXi IP address.
- If ESXi is using a self-signed certificate, verify that the host has been added to vCenter Server. This allows the authentication proxy server to trust ESXi.
- If ESXi is using a CA-signed certificate and is not provisioned by Auto Deploy, verify that the CA certificate has been added to the local trust certificate store of the authentication proxy server as described in the *vSphere Security* documentation.
- Authenticate the vSphere Authentication Proxy server to the host as described in the *vSphere Security* documentation.

Procedure

- 1 In the vSphere Client inventory, select the host.
- 2 Select the **Configuration** tab and click **Authentication Services**.
- 3 Click **Properties**.
- 4 In the Directory Services Configuration dialog box, select the directory server from the drop-down menu.
- 5 Enter a domain.
Use the form **name.tld** or **name.tld/container/path**.
- 6 Select the **Use vSphere Authentication Proxy** check box.
- 7 Enter the IP address of the authentication proxy server.
- 8 Click **Join Domain**.
- 9 Click **OK**.

View Directory Service Settings

You can view the type of directory server, if any, the host uses to authenticate users and the directory server settings.

Procedure

- 1 Select a host in the vSphere Client inventory, and click the **Configuration** tab.
- 2 Under Software, select **Authentication Services**.

The Authentication Services Settings page displays the directory service and domain settings.

Creating a Virtual Machine in the vSphere Client

8

Virtual machines are the key component in a virtual infrastructure. You can create virtual machines to add to the host inventory.

When you create a virtual machine, you associate it to a particular datastore and select an operating system and virtual hardware options. After you turn on the virtual machine, it consumes resources dynamically as the workload increases, or it returns resources dynamically as the workload decreases.

Every virtual machine has virtual devices that provide the same function as physical hardware. A virtual machine gets CPU and memory, access to storage, and network connectivity from the host it runs on.

This chapter includes the following topics:

- [“Start the Virtual Machine Creation Process in the vSphere Client,”](#) on page 43
- [“Select a Configuration Option for the New Virtual Machine in the vSphere Client,”](#) on page 44
- [“Enter a Name and Location for the Virtual Machine in the vSphere Client,”](#) on page 45
- [“Select a Datastore in the vSphere Client,”](#) on page 45
- [“Select a Virtual Machine Version in the vSphere Client,”](#) on page 46
- [“Select an Operating System in the vSphere Client,”](#) on page 46
- [“Select the Number of Virtual CPUs in the vSphere Client,”](#) on page 47
- [“Configure Virtual Memory in the vSphere Client,”](#) on page 47
- [“Configure Networks in the vSphere Client,”](#) on page 48
- [“Select a SCSI Controller in the vSphere Client,”](#) on page 49
- [“Selecting a Virtual Disk Type,”](#) on page 49
- [“Complete Virtual Machine Creation in the vSphere Client,”](#) on page 53

Start the Virtual Machine Creation Process in the vSphere Client

You use the Create New Virtual Machine wizard to create a virtual machine to place in the vSphere inventory. You open the wizard from the vSphere Client.

The selections you make in the New Virtual Machine wizard are not saved until you click **Finish** on the Ready to Complete page. If you cancel the wizard without completing all tasks, you cannot resume the wizard where you left off. You must start a new creation task.

You can create a new virtual machine in a datacenter, host, cluster, resource pool, or virtual machine folder.

Prerequisites

Verify that you have the following privileges:

- **Host.Local operations.Create virtual machine**
- **Virtual machine.Inventory.Create new** on the destination folder or datacenter.
- **Virtual machine.Configuration.Add new disk** on the destination folder or datacenter, if you are adding a new disk.
- **Virtual machine.Configuration.Add existing disk** on the destination folder or datacenter, if you are adding an existing disk.
- **Virtual machine.Configuration.Raw device** on the destination folder or datacenter, if you are using a RDM or SCSI pass-through device.
- **Virtual Machine.Configuration.Network**
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network that the virtual machine will be assigned to.

Procedure

- 1 Display the inventory objects in the vSphere Client by using the **Host and Clusters** view or the **VM and Templates** view.
- 2 Right-click an object and select **New > Virtual Machine**.

The New Virtual Machine wizard opens.

What to do next

Select a **Typical** or **Custom** configuration option in the New Virtual Machine wizard.

Select a Configuration Option for the New Virtual Machine in the vSphere Client

The **Typical** option shortens the virtual machine creation process by skipping choices that you rarely need to change from their defaults. The **Custom** option provides more flexibility and choices.

Several relationships affect the information that you must provide during virtual machine creation. These relationships include the inventory object on which you place the virtual machine, the customization path option you select, the datastore on which the virtual machine and its files reside, and the host or cluster on which it runs.

If you select a **Typical** configuration, the virtual machine hardware version defaults to that of the host on which you place the virtual machine. If you select a **Custom** configuration, you can accept the default or select an earlier hardware version. This configuration is useful if maintaining compatibility with an earlier version of an ESX/ESXi host is necessary.

Prerequisites

For a **Typical** configuration, verify that you have the following information:

- Virtual machine name and inventory location.
- Location in which to place the virtual machine (cluster, host, resource pool).
- Datastore on which to store the virtual machine's files.
- Guest operating system and version.

- Parameters for the virtual disk size and provisioning settings.

In addition to the information for a **Typical** configuration, for a **Custom** configuration, verify that you have the following information:

- Virtual machine version.
- Number of CPUs and memory size.
- Number of NICs, network to connect to, and network adapter types.
- SCSI controller type.
- Disk type (new disk, existing disk, RDM, or no disk).

Procedure

- 1 On the Configuration page of the New Virtual Machine wizard, select an option for creating the virtual machine.
- 2 Click **Next**.

The Name and Location page appears.

What to do next

Select a name and location for the virtual machine.

Enter a Name and Location for the Virtual Machine in the vSphere Client

The name you enter is used as the virtual machine's base name in the inventory. It is also used as the name of the virtual machine's files.

The name can be up to 80 characters long. Names are not case-sensitive, so the name `my_vm` is identical to `My_Vm`.

Prerequisites

Verify that you have an appropriate naming strategy in place.

Procedure

- 1 On the Name and Location page of the New Virtual Machine wizard, type a name.
- 2 Select a folder or the root of the datacenter.
- 3 Click **Next**.

The Host / Cluster or the Resource Pool page opens.

Select a Datastore in the vSphere Client

Datastores are logical containers that hide specifics of each storage device and provide a uniform model for storing virtual machine files. You can use datastores to store ISO images and virtual machine templates.

You can select from datastores already configured on the destination host or cluster.

Procedure

- 1 On the Storage page of the New Virtual Machine wizard, select a datastore in which to store the virtual machine files.
- 2 (Optional) To turn off Storage DRS for the virtual machine, select **Disable Storage DRS for this virtual machine**.

- 3 (Optional) Apply a virtual machine storage profile from the **VM Storage Profile** drop-down menu.

Select a datastore that is compatible with the virtual machine storage profile and large enough to hold the virtual machine and all of its virtual disk files.

The list of datastores shows which datastores are compatible with the selected virtual machine storage profile.

- 4 Click **Next**.

If you selected a Typical configuration path, the Guest Operating System page appears. If you selected a Custom configuration path, the Virtual Machine Version page appears.

Select a Virtual Machine Version in the vSphere Client

If the host or cluster where you place the virtual machine supports more than one VMware virtual machine version, you can select a version for the virtual machine.

For virtual machine and host compatibility options, see [“Virtual Machine Hardware Versions,”](#) on page 60.

Procedure

- 1 Select a virtual machine hardware version.

Option	Description
Virtual machine version 8	Compatible with ESXi 5.0 and later hosts. Provides the latest virtual machine features. Recommended for virtual machines that do not need to migrate to ESX/ESXi 4.x hosts.
Virtual machine version 7	Compatible with ESX/ESXi 4, 4.x and 5.0 hosts. Recommended for sharing storage or virtual machines with ESX/ESXi versions 3.5 to 4.1.
Virtual machine version 4	Compatible with ESX/ESXi 4.0 and later hosts. Recommended for virtual machines that need to run on ESX/ESXi 4 hosts.

- 2 Click **Next**.

The Guest Operating System page opens.

What to do next

Select a guest operating system for the virtual machine.

Select an Operating System in the vSphere Client

The guest operating system that you select affects the supported devices and number of virtual CPUs available to the virtual machine.

The New Virtual Machine wizard does not install the guest operating system. The wizard uses this information to select appropriate default values, such as the amount of memory needed.

When you select a guest operating system, BIOS or Extensible Firmware Interface (EFI) is selected by default, depending on the firmware supported by the operating system. Mac OS X Server guest operating systems support only EFI. If the operating system supports BIOS and EFI, you can change the default from the Options tab of the Virtual Machine Properties editor after you create the virtual machine and before you install the guest operating system. If you select EFI, you cannot boot an operating system that supports only BIOS, and the reverse.

IMPORTANT Do not change the firmware after the guest operating system is installed.

The Mac OS X Server must run on Apple hardware. You cannot power on a Mac OS X Server if it is running on other hardware.

Procedure

- 1 On the Guest Operating System page of the New Virtual Machine wizard, select an operating system family.
- 2 Select an operating system and version from the drop-down menu and click **Next**.
If you selected a Novell NetWare guest operating system, the Memory page opens. If any of the total cores available on the host, the maximum virtual CPUs supported by the virtual machine hardware version, or the maximum supported CPUs on the guest operating system equal 1, the virtual machine CPU count is set to 1 and the Memory page opens.
- 3 If you selected **Other (32-bit)** or **Other (64-bit)**, enter a name for the operating system in the text box.
- 4 Click **Next**.

What to do next

You can add memory or CPUs for the virtual machine.

Select the Number of Virtual CPUs in the vSphere Client

You can configure a virtual machine to have up to 32 virtual CPUs. The number of licensed CPUs on the host, the number of CPUs that the guest operating system supports, and the virtual machine hardware version determine the number of virtual CPUs that you can add.

VMware Virtual Symmetric Multiprocessing (Virtual SMP) enables a single virtual machine to use multiple physical processors simultaneously. You must have Virtual SMP to power on multiprocessor virtual machines.

Procedure

- 1 On the CPUs page of the New Virtual Machine wizard, select a value from the **Number of virtual sockets** drop-down menu.
- 2 Select a value from the **Number of cores per socket** drop-down menu.
To determine the total number of cores, multiply the number of cores per socket by the number of virtual sockets. The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.
The total number of cores appears.
- 3 Click **Next**.
The Memory page opens.

What to do next

Select the memory for the virtual machine.

Configure Virtual Memory in the vSphere Client

The amount of memory that you allocate for a virtual machine is the amount of memory that the guest operating system detects.

Minimum memory size is 4MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96MB of RAM or they cannot power on.

Maximum memory size for a virtual machine depends on the host's physical memory and the virtual machine's hardware version.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The memory size must be a multiple of 4MB. The maximum for best performance represents the threshold above which the host's physical memory is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

Table 8-1. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Version	Maximum Memory Size
ESXi 5.0	8	1011GB
ESX/ESXi 4.x	7	255GB
ESX/ESXi 3.x	4	65,532MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a version 4 virtual machine running on ESXi 5.0 is restricted to 65,532MB.

Procedure

- 1 On the Memory page of the New Virtual Machine wizard, select a size for the virtual memory.
You can use the slider or use the up and down arrows to select the number. To access the predefined default or recommended setting, click the colored triangles on the right-hand side of the memory bar.
- 2 Click **Next**.
The Network page opens.

What to do next

Select network adapters for the virtual machine.

Configure Networks in the vSphere Client

You can select the virtual network interface cards (NICs) to create on the virtual machine so that the virtual machine can communicate with other hosts and virtual machines. For each NIC, select the network and adapter type.



CAUTION Because virtual machines share their physical network hardware with the host, the accidental or malicious bridging of two networks by a virtual machine can occur. Spanning Tree protocol cannot protect against these occurrences.

You can select only four NICs during virtual machine creation. You can add more virtual NICs by selecting **Edit the virtual machine settings before completion** on the Ready to Complete page of the wizard, or by editing the virtual machine after it is created.

For more information about networking, see the *vSphere Networking* documentation.

Procedure

- 1 On the Network page of the New Virtual Machine wizard, select the number of NICs to connect from the drop-down menu.
- 2 For each NIC, select a network and adapter type from the drop-down menus.
Depending on the host version and the guest operating system, a choice of adapter types for each virtual NIC might not be available. In many cases, only one type of adapter is supported. If more than one type of adapter is supported, the recommended type for the guest operating system is selected by default.
- 3 (Optional) Click **Connect at Power On** to connect the NIC when the virtual machine is powered on.

- 4 Click **Next** to add a SCSI Controller.

Select a SCSI Controller in the vSphere Client

To access virtual disks, a virtual machine uses virtual SCSI controllers. Each virtual disk that a virtual machine can access through one of the virtual SCSI controllers resides in the VMFS datastore, NFS-based datastore, or on a raw disk. The choice of SCSI controller does not affect whether your virtual disk is an IDE or SCSI disk.

The wizard preselects the correct default controller based on the guest operation system you selected on the Guest Operating System page.

LSI Logic SAS and VMware Paravirtual controllers are available only for virtual machines with hardware version 7 or later. For details about VMware Paravirtual controllers, including conditions for use and limitations, see [About VMware Paravirtual SCSI Controllers](#).

Disks with snapshots might not experience performance gains when used on LSI Logic SAS and LSI Logic Parallel controllers.

Procedure

- 1 On the SCSI Controller page of the New Virtual Machine wizard, accept the default or select a SCSI controller type.
 - BusLogic Parallel
 - LSI Logic Parallel
 - LSI Logic SAS
 - VMware Paravirtual
- 2 Click **Next**.
The Select a Disk page opens.

What to do next

Select a disk on which to store the guest operating system files and data.

Selecting a Virtual Disk Type

You can create a virtual disk, use an existing virtual disk, or create Raw Device Mappings (RDMs), which give your virtual disk direct access to SAN. A virtual disk comprises one or more files on the file system that appear as a single hard disk to the guest operating system. These disks are portable among hosts.

You use the Create Virtual Machine wizard to add virtual disks during virtual machine creation. To add disks later, select the **Do Not Create Disk** option and use the Add Hardware wizard in the Virtual Machine Properties dialog box.

NOTE You cannot reassign virtual disks to a different controller type.

You can select from the following options:

- [Create a Virtual Disk in the vSphere Client](#) on page 50
When you create a virtual disk, you can specify disk properties such as size, format, clustering features, and more.
- [Use an Existing Virtual Disk in the vSphere Client](#) on page 51
You can use an existing disk that is configured with an operating system or other virtual machine data. This choice allows you to freely move the virtual hard drive from virtual machine to virtual machine.

- [Add an RDM Disk to a Virtual Machine in the vSphere Client](#) on page 52

You can store virtual machine data directly on a SAN LUN instead of storing it in a virtual disk file. This ability is useful if you are running applications in your virtual machines that must detect the physical characteristics of the storage device. Mapping a SAN LUN allows you to use existing SAN commands to manage storage for the disk.

Create a Virtual Disk in the vSphere Client

When you create a virtual disk, you can specify disk properties such as size, format, clustering features, and more.

For detailed information about disk types, see [“About Virtual Disk Provisioning Policies,”](#) on page 81.

Procedure

- 1 On the Create a Disk page of the New Virtual Machine wizard, select the disk size.
You can increase the disk size later or add disks in the Virtual Machine Properties dialog box.
- 2 Select the format for the virtual machine's disks and click **Next**.

Option	Action
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

- 3 Select a location to store the virtual disk files and click **Next**.

Option	Description
Store with the virtual machine	Stores the files with the configuration and other virtual machine files. This option makes file management easier.
Specify a datastore or datastore cluster	Stores the file separately from other virtual machine files.

The Advanced Options page opens.

- 4 Accept the default or select a different virtual device node.
In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

- 5 (Optional) To change the way disks are affected by snapshots, click **Independent** and select an option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 6 Click **Next**.

Your changes are recorded and the Ready to Complete page opens.

What to do next

View the selections for your virtual machine on the Ready to Complete page.

Use an Existing Virtual Disk in the vSphere Client

You can use an existing disk that is configured with an operating system or other virtual machine data. This choice allows you to freely move the virtual hard drive from virtual machine to virtual machine.

Procedure

- 1 On the Select Existing Disk page of the New Virtual Machine wizard, browse for a virtual disk file, click **OK**, and click **Next**.
- 2 Accept the default or select a different virtual device node.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

- 3 (Optional) To change the way disks are affected by snapshots, click **Independent** and select an option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 4 Click **Next**.

Your changes are recorded and the Ready to Complete page opens.

What to do next

Review the virtual machine configuration.

Add an RDM Disk to a Virtual Machine in the vSphere Client

You can store virtual machine data directly on a SAN LUN instead of storing it in a virtual disk file. This ability is useful if you are running applications in your virtual machines that must detect the physical characteristics of the storage device. Mapping a SAN LUN allows you to use existing SAN commands to manage storage for the disk.

When you map a LUN to a VMFS volume, vCenter Server creates a Raw Device Mapping (RDM) file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server to lock the LUN so that only one virtual machine can write to it at a time. For details about RDM, see the *vSphere Storage* documentation.

The RDM file has a .vmdk extension, but the file contains only disk information that describes the mapping to the LUN on the ESXi host. The actual data is stored on the LUN.

You can create the RDM as an initial disk for a new virtual machine or add it to an existing virtual machine. When you create the RDM, you specify the LUN to be mapped and the datastore on which to put the RDM.

NOTE You cannot deploy a virtual machine from a template and store its data on a LUN. You can only store its data in a virtual disk file.

Procedure

- 1 On the Select a Disk page of the New Virtual Machine wizard, select **Raw Device Mapping** and click **Next**.
- 2 From the list of SAN disks or LUNs, select a LUN for your virtual machine to access directly and click **Next**.
- 3 Select a datastore for the LUN mapping file and click **Next**.

You can place the RDM file on the same datastore where your virtual machine configuration file resides, or select a different datastore.

NOTE To use vMotion for virtual machines with enabled NPIV, make sure that the RDM files of the virtual machines are located on the same datastore. You cannot perform Storage vMotion or vMotion between datastores when NPIV is enabled.

- 4 Select a compatibility mode and click **Next**.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
Virtual	Allows the RDM to behave as if it were a virtual disk, so you can use such features as taking a snapshot, cloning, and so on. When you clone the disk or make a template from it, the contents of the LUN are copied into a .vmdk virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN into a virtual disk.

- 5 Accept the default or select a different virtual device node.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

- 6 (Optional) To change the way disks are affected by snapshots, click **Independent** and select an option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 7 Click **Next**.

Your changes are recorded and the Ready to Complete page opens.

What to do next

Review the virtual machine configuration.

Complete Virtual Machine Creation in the vSphere Client

The Ready to Complete page lets you review the configuration selections that you made for the virtual machine. You can change existing settings, configure resources, add hardware, and more.

You can configure additional virtual machine settings before or after completing the wizard.

Procedure

- 1 On the Ready to Complete page of the New Virtual Machine wizard, review the configuration settings for the virtual machine.
- 2 (Optional) Select **Edit the virtual machine settings before completion** and click **Continue**.

The Virtual Machine Properties editor opens. After you complete your changes and click **Finish**, both the Virtual Machine Properties editor and the New Virtual Machine wizard close. You cannot go back to review the wizard settings unless you click **Cancel**.

- 3 (Optional) Click **Cancel** to go back and review the wizard settings.
- 4 Click **Finish** to complete the creation task and close the wizard.

The virtual machine appears in the vSphere Client **Inventory** view.

What to do next

Before you can use the new virtual machine, you must partition and format the virtual drive, install a guest operating system, and install VMware Tools. Typically, the operating system's installation program handles partitioning and formatting the virtual drive.

Deploying OVF Templates

The VMware vSphere Client (vSphere Client) allows you to deploy and export virtual machines, virtual appliances, and vApps stored in Open Virtual Machine Format (OVF). An appliance is a pre-configured virtual machine that typically includes a preinstalled guest operating system and other software.

Deploying an OVF template allows you to add pre-configured virtual machines to your vCenter Server or ESXi inventory. Deploying an OVF template is similar to deploying a virtual machine from a template. However, you can deploy an OVF template from any local file system accessible from the vSphere Client machine, or from a remote web server. The local file systems can include local disks (such as C:), removable media (such as CDs or USB keychain drives), and shared network drives.

Exporting OVF templates allows you to create virtual appliances that can be imported by other users. You can use the export function to distribute pre-installed software as a virtual appliance, or as a means of distributing template virtual machines to users, including users who cannot directly access and use the templates in your vCenter Server inventory.

This chapter includes the following topics:

- [“Deploy an OVF Template,”](#) on page 55
- [“Browse VMware Virtual Appliance Marketplace,”](#) on page 57
- [“Export an OVF Template,”](#) on page 57

Deploy an OVF Template

When you connect directly to a host with the vSphere Client, you can deploy an OVF template from a local file system accessible to the vSphere Client machine, or from a web URL.

Procedure

- 1 In the vSphere Client, select **File > Deploy OVF Template**.

The Deploy OVF Template wizard appears.

- 2 Specify the source location and click **Next**.

Option	Action
Deploy from File	Browse your file system for an OVF or OVA template.
Deploy from URL	Specify a URL to an OVF template located on the internet. Example: http://vmware.com/MTN/appliance.ovf

- 3 View the OVF Template Details page and click **Next**.
- 4 If license agreements are packaged with the OVF template, the End User License Agreement page appears. Agree to accept the terms of the licenses and click **Next**.

- 5 Select the deployment configuration from the drop-down menu and click **Next**.

The option selected typically controls the memory settings, number of CPUs and reservations, and application-level configuration parameters.

Note This page appears only if the OVF template contains deployment options.

- 6 Select a datastore to store the deployed OVF template, and click **Next**.

Datastores are a unifying abstraction for storage locations such as Fibre Channel, iSCSI LUNs, or NAS volumes. On this page, you select from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

- 7 Select the disk format to store the virtual machine virtual disks, and click **Next**.

Format	Description
Thick Provisioned Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format the data remaining on the physical device is zeroed out when the virtual disk is created. it might take much longer to create disks in this format than to create other types o disks.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

- 8 If the appliance that you are deploying has one ore more vService dependencies, select a binding service provider.
- 9 For each network specified in the OVF template, select a network by right-clicking the **Destination Network** column in your infrastructure to set up the network mapping and click **Next**.
- 10 On the **IP Allocation** page, configure how IP addresses are allocated for the virtual appliance and click **Next**.

Option	Description
Fixed	You will be prompted to enter the IP addresses in the Appliance Properties page.
Transient	IP addresses are allocated from a specified range when the appliance is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses.

This page does not appear if the deployed OVF template does not contain information about the IP scheme it supports.

- 11 Set the user-configurable properties and click **Next**.

The set of properties that you are prompted to enter depend on the selected IP allocation scheme. For example, you are prompted for IP related information for the deployed virtual machines only in the case of a fixed IP allocation scheme.

- 12 Review your settings and click **Finish**.

The progress of the import task appears in the vSphere Client Status panel.

Browse VMware Virtual Appliance Marketplace

The Virtual Appliance Marketplace contains a variety of virtual appliances packaged in OVF format that you can download and deploy. Available vApps appear in the main panel.

To get to the Virtual Appliance Marketplace page, select **File > Browse VA Marketplace** from the main menu.

Procedure

- ◆ Select an available vApp and click **Download Now**.

The OVF Template Details page appears.

Export an OVF Template

An OVF package captures the state of a virtual machine or vApp into a self-contained package. The disk files are stored in a compressed, sparse format.

Required privilege: **vApp.Export**

Procedure

- 1 Select the virtual machine or vApp and select **File > Export > Export OVF Template**.

- 2 In the Export OVF Template dialog, type the **Name** of the template.

For example, type **MyVm**.

NOTE When exporting an OVF template with a name that contains asterisk (*) characters, those characters turn into underscore characters (_).

- 3 Enter the **Directory** location where the exported virtual machine template is saved, or click “...” to browse for the location.

The C:\ drive is the default location where the template is stored.

For example, **OvfLib**.

- 4 In the **Format** field, determine how you want to store the files.

- Select **Folder of files (OVF)** to store the OVF template as a set of files (.ovf, .vmdk, and .mf) This format is optimal if you plan to publish the OVF files on a web server or image library. The package can be imported, for example, into the vSphere client by publishing the URL to the .ovf file.
- Select **Single file (OVA)** to package the OVF template into a single .ova file. This might be convenient to distribute the OVF package as a single file if it needs to be explicitly downloaded from a web site or moved around using a USB key.

- 5 In **Description**, type a description for the virtual machine.

By default, the text from the **Notes** pane on the virtual machine’s **Summary** tab appears in this text box.

- 6 Select the checkbox if you want to include image files attached to floppy and CD/DVD devices in the OVF package.

NOTE This checkbox only shows if the virtual machine is connected to an ISO file or if the floppy drive is connected to a floppy image.

- 7 Click **OK**.

The download process is shown in the Export window.

Example: Folder Locations for OVF and OVA Files

If you type **0vfLib** for a new OVF folder, the following files might be created:

- C:\0vfLib\MyVm\MyVm.ovfI
- C:\0vfLib\MyVm.mf
- C:\0vfLib\MyVm-disk1.vmdk

If you type **C:\NewFolder\0vfLib** for a new OVF folder, the following files might be created:

- C:\NewFolder\0vfLib\MyVm\MyVm.ovfI
- C:\NewFolder\0vfLib\MyVm.mf
- C:\NewFolder\0vfLib\MyVm-disk1.vmdk

If you choose to export into the OVA format, and type **MyVm**, the file C:\MyVm.ova is created.

Configuring Virtual Machines in the vSphere Client

10

You can add or configure most virtual machine properties during the virtual machine creation process or after you create the virtual machine and install the guest operating system.

You configure virtual machines and change nearly every characteristic that you selected when you created the virtual machine.

You can configure three types of virtual machine properties.

Hardware	View existing hardware configuration and add or remove hardware.
Options	View and configure a number of virtual machine properties, such as power management interaction between the guest operating system and virtual machine, and VMware Tools settings.
Resources	Configure CPUs, CPU hyperthreading resources, memory and disks.

This chapter includes the following topics:

- [“Virtual Machine Hardware Versions,”](#) on page 60
- [“Locate the Hardware Version of a Virtual Machine in the vSphere Client,”](#) on page 61
- [“Change the Virtual Machine Name in the vSphere Client,”](#) on page 61
- [“View the Virtual Machine Configuration File Location in the vSphere Client,”](#) on page 62
- [“Edit Configuration File Parameters in the vSphere Client,”](#) on page 62
- [“Change the Configured Guest Operating System in the vSphere Client,”](#) on page 63
- [“Configure Virtual Machines to Automatically Upgrade VMware Tools,”](#) on page 63
- [“Virtual CPU Configuration,”](#) on page 64
- [“Virtual Memory Configuration,”](#) on page 70
- [“Network Virtual Machine Configuration,”](#) on page 74
- [“Parallel and Serial Port Configuration,”](#) on page 75
- [“Virtual Disk Configuration,”](#) on page 81
- [“Virtual Machine Controller Configuration,”](#) on page 86
- [“Other Virtual Machine Device Configuration,”](#) on page 89
- [“USB Configuration from an ESXi Host to a Virtual Machine,”](#) on page 95
- [“USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client,”](#) on page 100
- [“Add a Shared Smart Card Reader to Virtual Machines in the vSphere Client,”](#) on page 106

- [“Manage Power Management Settings for a Virtual Machine,”](#) on page 106
- [“Configure the Virtual Machine Power States,”](#) on page 107
- [“Delay the Boot Sequence in the vSphere Client,”](#) on page 108
- [“Enable Logging in the vSphere Client,”](#) on page 109
- [“Disable Acceleration in the vSphere Client,”](#) on page 109
- [“Configure Debugging and Statistics in the vSphere Client,”](#) on page 109

Virtual Machine Hardware Versions

The hardware version of a virtual machine reflects the virtual machine's supported virtual hardware features. These features correspond to the physical hardware available on the ESXi host on which you create the virtual machine. Virtual hardware features include BIOS and EFI, available virtual PCI slots, maximum number of CPUs, maximum memory configuration, and other characteristics typical to hardware.

When you create a virtual machine, you can accept the default hardware version, which corresponds to the host on which you create the virtual machine, or an earlier version. You can use an earlier hardware version in the following situations:

- To standardize testing and deployment in your virtual environment.
- If you do not need the capabilities of the newer version.
- To maintain compatibility with older hosts.

Virtual machines with hardware versions earlier than version 8 can run on ESXi 5.0 hosts, but do not have all the capabilities available in hardware version 8. For example, you cannot use 32 virtual processors or 1011GB of memory in virtual machines with hardware versions earlier than version 8.

The vSphere Web Client or the vSphere Client allows you to upgrade virtual machines only to the latest hardware version. If virtual machines do not have to stay compatible with older ESX/ESXi hosts, you can upgrade them on ESXi 5.0 hosts. In this case, they are upgraded to version 8.

- To maintain virtual machine compatibility with ESX/ESXi 3.5 hosts, upgrade the virtual machine on an ESX/ESXi 3.5 host, which results in a virtual machine upgrade to version 4.
- To maintain virtual machine compatibility with ESX/ESXi 4.x hosts, upgrade the virtual machine on an ESX/ESXi 4.x host, which results in a virtual machine upgrade to version 7.

A virtual machine can have an earlier hardware version than that of the host on which it runs in the following cases:

- You migrate a virtual machine created on an ESX/ESXi 4.x or earlier host to an ESXi 5.0 host.
- You create a virtual machine on an ESXi 5.0 host by using an existing virtual disk that was created on an ESX/ESXi 4.x or earlier host.
- You add a virtual disk created on an ESX/ESXi 4.x or earlier host to a virtual machine created on an ESXi 5.0 host.

You can create, edit, and run different virtual machine versions on a host if the host supports that version. Sometimes, virtual machine actions on a host are limited or the virtual machine has no access to the host.

Table 10-1. ESXi Hosts and Compatible Virtual Machine Hardware Versions

	Version 8	Version 7	Version 4	Compatible with vCenter Server Version
ESXi 5.0	Create, edit, run	Create, edit, run	Edit, run	vCenter Server 5.0
ESX/ESXi 4.x	Not supported	Create, edit, run	Create, edit, run	vCenter Server 4.x
ESX Server 3.x	Not supported	Not supported	Create, edit, run	VirtualCenter Server 2.x and later

Version 3 virtual machines are not supported on ESXi 5.0 hosts. To make full use of these virtual machines, upgrade the virtual hardware.

NOTE Virtual machine hardware version 4 might be listed as VM3 in documentation for earlier versions of ESX/ESXi.

Locate the Hardware Version of a Virtual Machine in the vSphere Client

You can locate the hardware version of a virtual machine by looking in the virtual machine **Summary** tab or the Virtual Machine Properties dialog box. You can also locate the hardware version for multiple virtual machines on the **Virtual Machine** tab of a datacenter, host, or cluster.

Procedure

- 1 In the vSphere Client inventory, select the virtual machine.
- 2 Select a method for viewing the version information.

Option	Description
Click the Summary tab.	The virtual machine hardware version appears under General on the virtual machine's Summary tab.
Right-click the virtual machine and select Edit Settings.	The virtual machine hardware version appears in the upper-right corner of the Virtual Machine Properties dialog box.
Select a datacenter, host, or cluster and click the Virtual Machine tab.	The virtual machine hardware version appears in the VM Version column. If the VM Version column is not displayed, right-click any column title and select VM Version.

Change the Virtual Machine Name in the vSphere Client

You can change the virtual machine name in the **Virtual Machine Name** panel in the Virtual Machine Properties dialog box.

Changing the name does not change the name of any virtual machine files or the name of the directory that the files are located in.

Prerequisites

- Verify that you are connected to the ESXi host on which the virtual machine runs.
- Verify that you have access to the virtual machine in the vSphere Client inventory list.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **General Options**.
- 3 Type a new name for the virtual machine.

- 4 Click **OK** to save your changes.

View the Virtual Machine Configuration File Location in the vSphere Client

You can view the location of the virtual machine configuration and working files. This information is useful when you are configuring backup systems.

Prerequisites

- Verify that you are connected to the vCenter Server or ESXi host on which the virtual machine runs.
- Verify that you have access to the virtual machine in the vSphere Client inventory list.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **General Options**.
- 3 Record the location of the configuration and working files and click **OK** to close the dialog box.

Edit Configuration File Parameters in the vSphere Client

You can change or add virtual machine configuration parameters if you intend to use experimental features or when instructed by a VMware technical support representative.

You also might see VMware documentation that instructs you to change or add a parameter. In such cases, you can safely follow the recommended procedure.

The following conditions apply:

- To change a parameter, you change the existing value for the keyword/value pair. For example, if you start with the keyword/value pair, keyword/value, and change it to keyword/value2, the result is keyword=value2.
- You cannot delete a configuration parameter entry.



CAUTION You must assign a value to configuration parameter keywords. If you don't assign a value, the keyword can return a value of 0, false, or disable, which can result in a virtual machine that cannot power on.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under Advanced, click **General**.
- 3 Click **Configuration Parameters**.
- 4 (Optional) Change or add a parameter.
- 5 Click **OK** to exit the Configuration Parameters dialog box.
- 6 Click **OK** to save your changes.

Change the Configured Guest Operating System in the vSphere Client

When you change the guest operating system type in the virtual machine settings, you change the setting for the guest operating system in the virtual machine's configuration file. To change the guest operating system itself, you must install the new operating system in the virtual machine.

When you set the guest operating system type for a new virtual machine, vCenter Server chooses configuration defaults based on the guest type. Changing the guest operating system type after the virtual machine is created does not retroactively change those settings. It affects the recommendations and setting ranges offered after the change.

Prerequisites

Power off the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **General Options**.
- 3 Select a guest operating system type and version.
- 4 Click **OK** to save your changes.

The virtual machine configuration parameters for the guest operating system are changed. You can now install the guest operating system.

Configure Virtual Machines to Automatically Upgrade VMware Tools

You can configure virtual machines to automatically update VMware Tools.

Note Automatic VMware Tools upgrade is not supported for virtual machines with Solaris or NetWare guest operating systems.

Prerequisites

- Verify that the virtual machines have a version of VMware Tools shipped with ESX/ESXi 3.5 or later installed.
- Verify that the virtual machines are hosted on ESX/ESXi 3.5 or later and vCenter Server 3.5 or later.
- Verify that the virtual machines are running a Linux or Windows guest OS that ESX/ESXi 3.5 or later and vCenter Server 3.5 or later support.

Procedure

- 1 Right-click the virtual machine and click **Edit Settings**.
- 2 Click the **Options** tab and select **VMware Tools**.
- 3 Select **Check and upgrade Tools during power cycling** in the **Advanced** pane.
- 4 Click **OK** to save your changes and close the dialog box.

The next time the virtual machine is powered on, it checks the ESX/ESXi host for a newer version of VMware Tools. If one is available, it is installed and the guest operating system is restarted (if required).

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters during virtual machine creation or after the guest operating system is installed. Some actions require you to power off the virtual machine before changing the settings.

VMware uses the following terminology. Understanding these terms can help you plan your CPU resource allocation strategy.

CPU	The CPU or processor is the portion of a computer system that carries out the instructions of a computer program and is the primary element carrying out the computer's functions. CPUs contain cores.
CPU Socket	A physical connector on a computer motherboard that accepts a single physical CPU. Many motherboards can have multiple sockets that can in turn accept multicore processors (CPUs). The vSphere Client computes the total number of cores to give the virtual machine from the number of virtual sockets and cores per socket that you select. The vSphere Web Client computes the total number of virtual sockets from the number of cores and cores per socket that you select.
Core	Comprises a unit containing an L1 cache and functional units needed to run programs. Cores can independently run programs or threads. One or more cores can exist on a single CPU.
Corelet	An AMD processor corelet is architecturally equivalent to a logical processor. Certain future AMD processors will comprise a number of compute units, where each compute unit has a number of corelets. Unlike a traditional processor core, a corelet lacks a complete set of private, dedicated execution resources. It shares some execution resources with other corelets such as an L1 Instruction Cache or a floating-point execution unit. AMD refers to corelets as cores, but because these are unlike traditional cores, VMware uses the nomenclature of "corelets" to make resource sharing more apparent.
Thread	Some cores can run independent streams of instructions simultaneously. In existing implementations, cores can run one or two software threads at one time by multiplexing the functional units of the core between the software threads, as necessary. Such cores are called dual or multithreaded.
Resource sharing	Shares specify the relative priority or importance of a virtual machine or resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources.
Resource allocation	You can change CPU resource allocation settings, such as shares, reservation, and limit, when available resource capacity does not meet demands. For example, if at year end the workload on accounting increases, you can increase the accounting resource pool reserve.
vSphere Virtual Symmetric Multiprocessing (Virtual SMP)	Feature that enables a single virtual machine to have multiple cores.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine depends on the number of logical CPUs on the host, the host license, and the type of guest operating system that is installed on the virtual machine.

Be aware of the following limitations:

- A virtual machine cannot have more virtual CPUs than the number of logical cores on the host. The number of logical cores is equal to the number of physical cores if hyperthreading is disabled or two times that number if hyperthreading is enabled.
- Not every guest operating system supports Virtual SMP, and some that do require reinstallation if the number of CPUs changes. For more information about using Virtual SMP, search the VMware Knowledge Base.
- Guest operating systems that support Virtual SMP might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide*.
- Hyperthreaded hosts might affect virtual machine performance, depending on the workload. The best practice is to test your workload to determine whether to enable or disable hyperthreading on your hosts.

Configuring Multicore Virtual CPUs

VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU's cores, which increases overall performance.

IMPORTANT When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

You can configure a virtual machine that runs on an ESXi host to have up to 64 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs is the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 64 logical CPUs, you can configure the virtual machine for 64 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

For more information about multicore CPUs, see the *vSphere Resource Management* documentation.

Change CPU Hot-Plug Settings in the vSphere Client

The CPU hot plug option lets you add CPU resources for a virtual machine while the machine is powered on.

The following conditions apply:

- For best results, use hardware version 8 virtual machines.
- Hot-adding multicore virtual CPUs is supported only with hardware version 8 virtual machines.
- Not all guest operating systems support CPU hot add. You can disable these settings if the guest is not supported.

- To use the CPU hot-add feature with hardware version 7 virtual machines, set **Number of cores per socket** to 1.
- Adding CPU resources to a running virtual machine with CPU hot plug enabled disconnects and reconnects all USB passthrough devices connected to that virtual machine.

Prerequisites

Verify that the virtual machine is running under the following conditions:

- VMware Tools is installed. This condition is required for hot plug functionality with Linux guest operating systems.
- The virtual machine has a guest operating system that supports CPU hot plug.
- The virtual machine is using hardware version 7 or later.
- The virtual machine is powered off.
- Required privileges: **Virtual Machine.Configuration.Settings** on the virtual machine

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under **Advanced**, select **Memory/CPU Hotplug**.
- 3 Change the CPU Hot Plug setting.
- 4 Click **OK** to save your changes.

What to do next

You can now add CPUs to the powered on virtual machine.

Change the Number of Virtual CPUs in the vSphere Client

You can configure a virtual machine that runs on an ESXi host to have up to 32 virtual CPUs. You can change the number of virtual CPUs while the virtual machine is running or powered off.

Virtual CPU hot add is supported for virtual machines with multicore CPU support that are running on hardware version 8 or later. When the virtual machine is powered on, and CPU hot add is enabled, you can hot add virtual CPUs to the running virtual machine. You can add only multiples of the number of cores per socket. For multicore CPUs, the host must have a license for vSphere Virtual Symmetric Multiprocessing (Virtual SMP).

IMPORTANT When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Prerequisites

- If CPU hot add is not enabled, power off the virtual machine before adding CPUs.
- If CPU hot remove is not enabled, power off the virtual machine before removing CPUs.
- To hot add multicore CPUs, verify that the virtual machine has hardware version 8.
- Required privilege: **Virtual Machine.Configuration.Change CPU Count** on the virtual machine

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **CPUs**.
- 3 Select a value from the **Number of virtual sockets** drop-down menu.

- 4 Select a value from the **Number of cores per socket** drop-down menu.

The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

- 5 Click **OK** to save your changes.

Example: Adding Multicore CPU Resources to a Virtual Machine

You might have the following existing CPU resources, which you configured for the virtual machine while you were creating it, or after you created it and it was in a powered off state.

CPU Resource Settings	Existing Value
Number of virtual sockets	2
Number of cores per socket	2
Total number of cores	4

With CPU hot plug enabled and the virtual machine running, you can select the number of sockets to add from the **Number of virtual sockets** drop-down menu. The **Number of cores per socket** drop-down menu is unavailable and retains a value of 2. If you select 3 virtual sockets, you are adding 1 socket with 2 cores so that the virtual machine has 6 virtual CPUs.

CPU Resource Settings	Existing Value	Hot-plug value
Number of virtual sockets	2	3
Number of cores per socket	2	2
Total Number of cores	4	6

Allocate CPU Resources in the vSphere Client

You can change the amount of CPU resources allocated to a virtual machine by using the shares, reservations, and limits settings.

A virtual machine has the following user-defined settings that affect its CPU resource allocation.

Limit	Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz.
Shares	Each virtual machine is granted a number of CPU shares. The more shares a virtual machine has, the more often it gets a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

Prerequisites

Required Privilege: **Virtual machine.Configuration.Change resource**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab and select **CPU**.

- 3 Allocate the CPU capacity for this virtual machine.

Option	Description
Shares	CPU shares for this virtual machine in relation to the parent's total. Sibling virtual machines share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each virtual machine a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this virtual machine.
Limit	Upper limit for this virtual machine's CPU allocation. Select Unlimited to specify no upper limit.

- 4 Click **OK** to save your changes.

Configuring Advanced CPU Scheduling Settings

You can select CPU options that involve scheduling the virtual machine processing to physical processor cores and hyperthreads. ESXi generally manages processor scheduling well, even when hyperthreading is enabled. These settings are useful only for detailed tweaking of critical virtual machines.

Configure Hyperthreaded Core Sharing in the vSphere Client

You can select how the virtual CPUs of a virtual machine share physical cores on a hyperthreaded system.

Hyperthreading technology allows a single physical processor to behave like two logical processors. The hyperthreaded core sharing option provides detailed control over whether to schedule a virtual machine to share a physical processor core. The processor can run two independent applications at the same time. Although hyperthreading does not double the performance of a system, it can increase performance by better utilizing idle resources.

Prerequisites

- The hyperthreaded core sharing option must be enabled in your system's BIOS settings. For more information, see the *Resource Management* documentation.
- Power off the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab and select **Advanced CPU**.
- 3 Select a mode from the **Hyperthreading Sharing Mode** drop-down menu.

Option	Description
Any (default)	The virtual CPUs of this virtual machine can share cores with other virtual CPUs of this or other virtual machines.
None	The virtual CPUs of this virtual machine have exclusive use of a processor core whenever they are scheduled to it. The other hyperthread of the core is halted while this virtual machine is using the core.
Internal	On a virtual machine with exactly two virtual processors, the two virtual processors are allowed to share one physical core (at the discretion of the host scheduler), but this virtual machine never shares a core with any other virtual machine. If this virtual machine has any other number of processors other than two, this setting is the same as the None setting.

- 4 Click **OK** to save your changes.

Configure Processor Scheduling Affinity in the vSphere Client

The **Scheduling Affinity** option gives you detailed control over how virtual machine CPUs are distributed across the host's physical cores (and hyperthreads if hyperthreading is enabled). This panel does not appear for virtual machines in a DRS cluster or when the host has only one processor core and no hyperthreading.

Using CPU affinity, you can assign a virtual machine to a specific processor. This assignment allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

For potential issues with CPU affinity, see the *Resource Management* documentation.

Prerequisites

Power off the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab and select **Advanced CPU**.
- 3 In the Scheduling Affinity panel, enter a comma-separated list of hyphenated processor ranges.
For example, "0,4-7" would indicate affinity with CPUs 0,4,5,6, and 7. Selecting all processors is identical to selecting no affinity. You must provide at least as many processor affinities as you have virtual CPUs.
- 4 Click **OK** to save your changes.

Change CPU Identification Mask Settings in the vSphere Client

CPU identification (CPU ID) masks control the CPU features visible to the virtual machine's guest operating system. Masking or hiding CPU features can make a virtual machine widely available to ESXi hosts for migration. vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migration with vMotion.

For example, masking the AMD No eXecute (NX) and the Intel eXecute Disable (XD) bits prevents the virtual machine from using these features, but provides compatibility that allows you to migrate virtual machines to ESXi hosts that do not include this capability. When the NX/XD bit is visible to the guest operating system, the virtual machine can use this feature, but you can migrate the virtual machine only to hosts on which the feature is enabled.

NOTE You rarely need to change the CPU identification mask configuration settings. Almost all changes are made only to the NX/XD bit.

See the *vCenter Server and Host Management* documentation for detailed information about vMotion compatibility and CPU masks.

Prerequisites

- Verify that you have access to the virtual machine in the vSphere Client inventory list.
- Power off the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under Advanced, select **CPUID Mask**.

- 3 In the **CPU Identification Mask** panel, select an NX flag option.

Option	Description
Hide the NX/XD flag from guest	Increases vMotion compatibility. Hiding the NX/XD flag increases vMotion compatibility between hosts, but might disable certain CPU security features.
Expose the NX/XD flag to guest	Keeps all CPU security features enabled.
Keep current Advanced setting values for the NX/XD flag	Uses the NX/XD flag settings specified in the CPU Identification Mask dialog box. Enabled only when current settings specify something other than what is specified in the other NX/XD flag options, for example, if the NX/XD flag bit setting varies with processor brand.

- 4 (Optional) To edit mask values other than the NX bit or to set NX mask values to states other than “0” or “H”, click **Advanced**.
 - a Select the relevant tab.
 - b Click a row and edit the mask value.
To view an explanation of a values symbol, click **Legend**.
 - c Click **OK** to apply the changes and return to the Virtual Machine Properties dialog box.
- 5 Click **OK** to save your changes.

Change CPU/MMU Virtualization Settings in the vSphere Client

ESXi can determine whether a virtual machine should use hardware support for virtualization. It makes this determination based on the processor type and the virtual machine. Overriding the automatic selection can provide better performance for some use cases.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under Advanced, select **CPU/MMU Virtualization**.
- 3 Select an instruction set.
 - **Automatic**
 - **Use only software virtualization**
 - **Use hardware support for CPU virtualization (VT/AMD-V) only**
 - **Use hardware support for both CPU and MMU virtualization (VT/AMD-V and EPT/RVI)**
- 4 Click **OK** to save your changes.

Virtual Memory Configuration

You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Some actions require that you power off the virtual machine before changing the settings.

The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size. ESXi hosts limit the memory resource use to the maximum amount useful for the virtual machine, so that you can accept the default of Unlimited memory resources.

Change the Memory Configuration in the vSphere Client

You can reconfigure the memory allocated to a virtual machine's hardware.

Minimum memory size is 4MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96MB of RAM or they cannot power on.

Maximum memory size for a virtual machine depends on the host's physical memory and the virtual machine's hardware version.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The memory size must be a multiple of 4MB. The maximum for best performance represents the threshold above which the host's physical memory is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

Table 10-2. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Version	Maximum Memory Size
ESXi 5.0	8	1011GB
ESX/ESXi 4.x	7	255GB
ESX/ESXi 3.x	4	65,532MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a version 4 virtual machine running on ESXi 5.0 is restricted to 65,532MB.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **Memory**.
- 3 Adjust the amount of memory allocated to the virtual machine.
- 4 Click **OK** to save your changes.

Allocate Memory Resources in the vSphere Client

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings.

A virtual machine has three user-defined settings that affect its memory resource allocation.

Limit	Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes.
Shares	Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the more often it gets a time slice of a memory when no memory idle time is present. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the <i>vSphere Resource Management</i> documentation.

Assigning a virtual machine a reservation larger than its configured memory is wasteful. The vSphere Client does not allow you to make such an assignment on the **Resources** tab. If you give a virtual machine a large reservation and then reduce its configured memory size on the **Hardware** tab, the reservation is reduced to match the new configured memory size. You must power off the virtual machine before configuring memory resources.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab and select **Memory**.
- 3 Allocated the memory capacity for this virtual machine.

Option	Description
Shares	The values Low , Normal , High , and Custom are compared to the sum of all shares of all virtual machines on the server. You can use share allocation symbolic values to configure their conversion into numeric values.
Reservation	Guaranteed memory allocation for this virtual machine.
Limit	Upper limit for this virtual machine's memory allocation.
Unlimited	No upper limit is specified.

- 4 Click **OK** to save your changes.

Change Memory Hot-Add Settings in the vSphere Client

Memory hot add lets you add memory resources for a virtual machine while the machine is powered on.

Prerequisites

- The virtual machine has a guest operating system that supports Memory hot add functionality.
- The virtual machine is using hardware version 7 or later.
- VMware Tools is installed.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under Advanced, select **Memory/CPU Hotplug**.
- 3 Enable or disable memory hot add.
 - **Enable memory hot add for this virtual machine.**
 - **Disable memory hot add for this virtual machine.**
- 4 Click **OK** to save your changes.

Associate Memory Allocations with a NUMA Node in the vSphere Client

You can specify that all future memory allocations on a virtual machine use pages associated with a single NUMA node (also known as manual memory affinity). When the virtual machine uses local memory, the performance improves on that virtual machine.

The following conditions apply to memory optimization with NUMA:

- The NUMA option is available on the Advanced Memory Resources page only if the host uses NUMA memory architecture.
- Affinity settings are meaningful only when used to modify the performance of a specific set of virtual machines on one host. This option is not available when the virtual machine resides on a DRS cluster. All affinity values are cleared when you move the virtual machine to a new host.

- You can specify nodes to use for future memory allocations only if you have also specified CPU affinity. If you make manual changes only to the memory affinity settings, automatic NUMA rebalancing does not work properly.
- Checking all the boxes is the same as applying no affinity.

For information about NUMA and advanced memory resources, including usage examples, see the *Resource Management* documentation.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Select the **Resources** tab, and select **Memory**.
- 3 In the **NUMA Memory Affinity** panel, set the NUMA node affinity for the virtual machine.
 - **No affinity**
 - **Use memory from nodes**
- 4 Click **OK** to save your changes.

Change the Swap File Location in the vSphere Client

When a virtual machine is powered on, the system creates a VMkernel swap file to serve as a backing store for the virtual machine's RAM contents. You can accept the default swap file location or save the file to a different location. By default, the swap file is stored in the same location as the virtual machine's configuration file.

For more information about host swap file settings, see the *vCenter Server and Host Management* documentation. For more information about cluster settings, see the *Resource Management* documentation.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Option** tab and under Advanced, select **Swapfile Location**.
- 3 Select an option.

Option	Description
Default	Stores the virtual machine swap file at the default location defined by the host or cluster swap file settings.
Always store with the virtual machine	Stores the virtual machine swap file in the same folder as the virtual machine configuration file.
Store in the host's swapfile datastore	Stores the virtual machine swap file in the swap file datastore defined by the host or cluster swap file settings.

- 4 Click **OK** to save your changes.

Network Virtual Machine Configuration

ESXi networking features provide communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines. The networking features also allow management of ESXi hosts and provide communication between VMkernel services (NFS, iSCSI, or vSphere vMotion) and the physical network. When you configure networking for a virtual machine, you select or change an adapter type, a network connection, and whether to connect the network when the virtual machine powers on.

Change the Virtual Network Adapter (NIC) Configuration in the vSphere Client

You can change the power-on connection setting, the MAC address, and the network connection for the virtual network adapter configuration for a virtual machine.

Prerequisites

Required Privileges:

- **Virtual machine.Configuration.Modify device settings** for editing the MAC address and network.
- **Virtual machine.Interaction.Device connection** for changing **Connect** and **Connect at power on**.
- **Network.Assign network**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the appropriate NIC in the Hardware list.
- 3 (Optional) To connect the virtual NIC when the virtual machine is powered on, select **Connect at power on**.
- 4 (Optional) Click the blue information icon under DirectPath I/O to view details regarding the virtual NIC's DirectPath I/O status and capability.
- 5 Select an option for MAC address configuration.

Option	Description
Automatic	vSphere assigns a MAC address automatically.
Manual	Type the MAC address to use.

- 6 Configure the **Network Connection** for the virtual NIC.

Option	Description
Standard settings	The virtual NIC connects to a standard or distributed port group. Select the port group for the virtual NIC to connect to from the Network label drop-down menu.
Advanced settings	<p>The virtual NIC connects to a specific port on a vSphere distributed switch. This option appears only when a vSphere distributed switch is available.</p> <ol style="list-style-type: none"> a Click Switch to advanced settings. b Select a vSphere distributed switch for the virtual NIC to use from the VDS drop-down menu. c Type the Port ID of the distributed port for virtual NIC to connect to.

- 7 Click **OK** to save your changes.

Add a Network Adapter to a Virtual Machine in the vSphere Client

When you add a Network adapter (NIC) to a virtual machine, you select the adapter type, the network connection, and whether the device should connect when the virtual machine is powered on.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select **Ethernet Adapter**, and click **Next**.
- 4 Select an adapter type from the drop-down menu.
- 5 In the Network connection panel, select either a named network with a specified label or a legacy network.
- 6 To connect the virtual NIC when the virtual machine is powered on, select **Connect at power on**.
- 7 Click **Next**.
- 8 Review your selections and click **Finish**.
- 9 Click **OK** to save your changes.

Parallel and Serial Port Configuration

Parallel and serial ports are interfaces for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port or to a file on the host computer. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can add parallel and serial ports and change the serial port configuration.

Using Serial Ports with vSphere Virtual Machines

You can set up virtual serial ports connections for vSphere virtual machines in several ways. The connection method that you select depends on the task that you need to accomplish.

You can set up virtual serial ports to send data in the following ways.

Physical serial port on the host	Sets the virtual machine to use a physical serial port on the host computer. This method lets you use an external modem or a hand-held device in a virtual machine.
Output to file	Sends output from the virtual serial port to a file on the host computer. This method lets you capture the data that a program running in the virtual machine sends to the virtual serial port.
Connect to a named pipe	Sets a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. With this method, two virtual machines or a virtual machine and a process on the host can communicate as if they were physical machines connected by a serial cable. For example, use this option for remote debugging on a virtual machine.
Connect over the network	Enables a serial connection to and from a virtual machine's serial port over the network. The Virtual Serial Port Concentrator (vSPC) aggregates traffic from multiple serial ports onto one management console. vSPC behavior is similar to physical serial port concentrators. Using a vSPC also allows

network connections to a virtual machine's serial ports to migrate seamlessly when you use vMotion to migrate the virtual machine. For requirements and steps to configure the Avocent ACS v6000 virtual serial port concentrator, see <http://kb.vmware.com/kb/1022303>.

Server and Client Connections for Named Pipe and Network Serial Ports

You can select a client or server connection for serial ports. Your selection determines whether the system waits for a connection or initiates it. Typically, to control a virtual machine over a serial port, you select a server connection. This selection lets you control the connections, which is useful if you connect to the virtual machine only occasionally. To use a serial port for logging, select a client connection. This selection lets the virtual machine connect to the logging server when the virtual machine starts and to disconnect when it stops.

Physical Serial Port Conditions

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the following conditions apply.

Supported	Not Supported
Serial ports that are integrated into the motherboard	Migration with vMotion
	Serial ports present on add-on expansion cards might be supported by PCI DirectPath I/O. See “Add a PCI Device in the vSphere Client,” on page 93.
	Serial ports connected through USB are not supported for serial port passthrough. They might be supported by USB passthrough from an ESXi host to a virtual machine. See USB Configuration from an ESXi Host to a Virtual Machine .

Adding a Firewall Rule Set for Serial Port Network Connections

If you add or configure a serial port that is backed by a remote network connection, ESXi firewall settings can prevent transmissions.

Before you connect network-backed virtual serial ports, you must add one of the following firewall rule sets to prevent the firewall from blocking communication:

- **VM serial port connected to vSPC.** Use to connect the serial port output through a network with the **Use virtual serial port concentrator** option enabled to allow only outgoing communication from the host.
- **VM serial port connected over network.** Use to connect the serial port output through a network without the virtual serial port concentrator.

IMPORTANT Do not change the allowed IP list for either rule set. Updates to the IP list can affect other network services that might be blocked by the firewall.

For details about allowing access to an ESXi service through the firewall, see the *vSphere Security* documentation.

Change the Serial Port Configuration in the vSphere Client

A virtual machine can use up to four virtual serial ports. You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer by using a host-side-named pipe. In addition, you can use a port or vSPC URI to connect a serial port over the network.

Virtual machines can be in a powered-on state during configuration.

Prerequisites

- Check that you know the correct media types for the port to access, vSPC connections, and any conditions that might apply. See [Using Serial Ports with vSphere Virtual Machines](#).
- To connect a serial port over a network, add a Firewall rule set. See [Adding a Firewall Rule Set for Serial Port Network Connections](#).
- Required privilege: **Virtual machine.Configuration.Device connection**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select a serial port in the Hardware list.
- 3 (Optional) Change the **Device status** settings.

Option	Description
Connected	Connects or disconnects the device while the virtual machine is running.
Connect at power on	Connects the device whenever you power on the virtual machine. You can change this setting when the virtual machine is either powered on or powered off.

- 4 Select a connection type.

Option	Action
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. <ol style="list-style-type: none"> a Type a name for the pipe in the Pipe Name field. b Select the Near end and Far end of the pipe from the drop-down menus.
Connect over the network	Select Use network to connect through a remote network. <ol style="list-style-type: none"> a Select the network backing. <ul style="list-style-type: none"> ■ Select Server to have the virtual machine monitor incoming connections from other hosts. ■ Select Client to have the virtual machine initiate a connection to another host. b Enter a Port URI. <p>The URI is the remote end of the serial port to which the virtual machine's serial port should connect.</p> c If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select Use Virtual Serial Port Concentrator and enter the vSPC URI location.

- 5 (Optional) Select **Yield on poll**.

Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

- 6 Click **OK** to save your changes.

Example: Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Add a Serial Port to a Virtual Machine in the vSphere Client

A virtual machine can use up to four virtual serial ports. You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side-named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network.

Prerequisites

- Verify that the virtual machine is powered off.
- Familiarize yourself with the media types for the port to access, vSPC connections, and any conditions that might apply. See [Using Serial Ports with vSphere Virtual Machines](#).
- To connect a serial port over a network, add a Firewall rule set. See [Adding a Firewall Rule Set for Serial Port Network Connections](#).
- Required privilege: **Virtual Machine .Configuration.Add or Remove Device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **Add**.
- 3 Select **Serial Port** and click **Next**.
- 4 On the Serial Port Type page, select the type of media for the port to access.

Option	Description
Use physical serial port on the host	Click Next and select the port from the drop-down menu.
Output to file	Click Next and browse to the location of the file on the host to store the output of the virtual serial port.

Option	Description
Connect to named pipe	<ol style="list-style-type: none"> Click Next and type a name for the pipe in the Pipe Name field. Select the Near end and Far end of the pipe from the drop-down menus.
Connect via network	<ol style="list-style-type: none"> Click Next and click Server or Client and type the Port URI. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select Use Virtual Serial Port Concentrator (vSPC) and type the vSPC URI location.

- (Optional) Deselect **Connect at power on** if you do not want the parallel port device to be connected when the virtual machine powers on.
- (Optional) Select **Yield on poll**.

Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.
- Review the information on the Ready to Complete page and click **Finish**.

Example: Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Change the Parallel Port Configuration in the vSphere Client

You can change the output file and schedule the parallel port to connect or disconnect when the virtual machine powers on.

You can use a parallel port on the virtual machine to send output to a file. You cannot use a physical parallel port on ESXi hosts.

Virtual machines can be powered on during the configuration

Procedure

- In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- Click the **Hardware** tab and select the parallel port to change.
- Select **Output to file** and click **Browse** to navigate to the file location.
- (Optional) Deselect **Connect at power on** if you do not want the parallel port device to be connected when the virtual machine powers on.
- Click **OK** to save your changes.

Add a Parallel Port to a Virtual Machine in the vSphere Client

You can use the Add Hardware wizard to add and configure a parallel port to send output to a file on the host computer.

Prerequisites

- Verify that the virtual machine is powered off.
- Required privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select **Parallel Port** and click **Next**.
- 4 Select **Output to file** and browse to the location of the file.
- 5 (Optional) Select or deselect the **Connected** check box to connect or disconnect the device.
- 6 Click **Next**.
- 7 Review the information on the Ready to Complete page, and click **Finish**.

Configure Fibre Channel NPIV Settings in the vSphere Client

N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers. This capability lets you control virtual machine access to LUNs on a per-virtual machine basis.

Each virtual port is identified by a pair of world wide names (WWNs): a world wide port name (WWPN) and a world wide node name (WWNN). These WWNs are assigned by vCenter Server.

For detailed information on how to configure NPIV for a virtual machine, see *vSphere Storage*.

NPIV support is subject to the following limitations:

- NPIV must be enabled on the SAN switch. Contact the switch vendor for information about enabling NPIV on their devices.
- NPIV is supported only for virtual machines with RDM disks. Virtual machines with regular virtual disks continue to use the WWNs of the host's physical HBAs.
- The physical HBAs on the ESXi host must have access to a LUN using its WWNs in order for any virtual machines on that host to have access to that LUN using their NPIV WWNs. Ensure that access is provided to both the host and the virtual machines.
- The physical HBAs on the ESXi host must support NPIV. If the physical HBAs do not support NPIV, the virtual machines running on that host will fall back to using the WWNs of the host's physical HBAs for LUN access.
- Each virtual machine can have up to 4 virtual ports. NPIV-enabled virtual machines are assigned exactly 4 NPIV-related WWNs, which are used to communicate with physical HBAs through virtual ports. Therefore, virtual machines can utilize up to 4 physical HBAs for NPIV purposes.

You can view or edit the virtual machines WWNs on the **Options** tab.

Prerequisites

- To edit the virtual machine's WWNs, power off the virtual machine.
- Verify that the virtual machine has a datastore containing a LUN that is available to the host.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under **Advanced** select **Fibre Channel NPIV**.
- 3 (Optional) Select the **Temporarily Disable NPIV for this virtual machine** check box.
- 4 Assigned WWNs appear in the WWN Assignments panel.
 - To leave WWNs unchanged, select **Leave unchanged**.
 - To have the ESXi host generate new WWNs, select **Generate New WWNs**.
 - To remove the current WWN assignments, select **Remove WWN assignment**.
- 5 Click **OK** to save your changes.
- 6 Provide the WWN assignments to your SAN administrator.

The administrator needs the assignments to configure virtual machine access to the LUN.

Virtual Disk Configuration

You can add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the virtual machine is running. You can set most of the virtual disk parameters during virtual machine creation or after you install the guest operating system.

You can store virtual machine data in a new virtual disk, an existing virtual disk, or a mapped SAN LUN. A virtual disk, which appears as a single hard disk to the guest operating system, is composed of one or more files on the host file system. You can copy or move virtual disks on the same hosts or between hosts.

For virtual machines running on an ESXi host, you can store the virtual machine data directly on a SAN LUN instead of storing it in a virtual disk file. This ability is useful if you are running applications in your virtual machines that must detect the physical characteristics of the storage device. Additionally, mapping a SAN LUN allows you to use existing SAN commands to manage storage for the disk.

When you map a LUN to a VMFS volume, vCenter Server or the ESXi host creates a raw device mapping (RDM) file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server or the ESXi host to lock the LUN so that only one virtual machine can write to it. This file has a `.vmdk` extension, but the file contains only disk information that describes the mapping to the LUN on the ESXi system. The actual data is stored on the LUN. You cannot deploy a virtual machine from a template and store its data on a LUN. You can store only its data in a virtual disk file.

About Virtual Disk Provisioning Policies

When you perform certain virtual machine management operations, such as creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine, you can specify a provisioning policy for the virtual disk file.

NFS datastores with Hardware Acceleration and VMFS datastores support the following disk provisioning policies. On NFS datastores that do not support Hardware Acceleration, only thin format is available.

You can use Storage vMotion or cross-host Storage vMotion to transform virtual disks from one format to another.

Thick Provision Lazy Zeroed

Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Virtual machines do not read stale data from the physical device.

Thick Provision Eager Zeroed

A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks.

Thin Provision

Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it.

Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.

NOTE If a virtual disk supports clustering solutions such as Fault Tolerance, do not make the disk thin.

You can manually inflate the thin disk, so that it occupies the entire provisioned space. If physical storage space is exhausted and the thin provisioned disk cannot grow, the virtual machine becomes unusable.

Change the Virtual Disk Configuration in the vSphere Client

You can change the virtual device node, the size of the disk, and the persistence mode for virtual disk configuration for a virtual machine.

NOTE The Manage Paths feature for RDM disks is not available for virtual machines on legacy hosts running versions of ESX Server earlier than 3.0.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the hard disk to modify.
The name of the disk file and the disk type (thick or thin) appear in the upper-right pane.
- 3 Select a **Virtual Device Node** type from the drop-down menu.
- 4 To change the size of the disk, enter a new value in the **Provisioned Size** text box.

- 5 (Optional) To change the way disks are affected by snapshots, click **Independent** and select an option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 6 Click **OK** to save your changes.

Add a Hard Disk to a Virtual Machine in the vSphere Client

When you add a hard disk to a virtual machine, you can create a new virtual disk, add an existing virtual disk, or add a mapped SAN LUN.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and use a Buslogic controller with bus sharing turned on to share a data disk with another virtual machine.

NOTE You cannot use migration with vMotion to migrate virtual machines that use raw disks for clustering purposes.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select **Hard Disk** and click **Next**.

- 4 Select the type of disk to use.

Option	Action
Create a new virtual disk	<p>a Type the disk capacity.</p> <p>b Select a disk format.</p> <ul style="list-style-type: none"> ■ Thick Provision Lazy Zeroed creates a virtual disk in a default thick format. ■ Thick Provision Eager Zeroed creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. ■ Thin Provision creates a disk in thin format. Use this format to save storage space. <p>c Select a location to store the disk. Store with the virtual machine or Specify a datastore.</p> <p>d If you selected Specify a datastore, browse for the datastore location, and click Next.</p>
Use an Existing Virtual Disk	Browse for the disk file path and click Next .
Raw Device Mappings	<p>Gives your virtual machine direct access to SAN.</p> <p>a Select the LUN to use for the raw disk, and click Next.</p> <p>b Select the datastore and click Next.</p> <p>c Select the compatibility mode.</p> <ul style="list-style-type: none"> ■ Physical allows the guest operating system to access the hardware directly. ■ Virtual allows the virtual machine to use VMware snapshots and other advanced functions. <p>d Click Next.</p>

- 5 Accept the default or select a different virtual device node.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

- 6 (Optional) To change the way disks are affected by snapshots, click **Independent** and select an option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 7 Click **Next**.
- 8 Review the information and click **Finish**.
- 9 Click **OK** to save your changes.

Use Disk Shares to Prioritize Virtual Machines in the vSphere Client

You can change the disk resources for a virtual machine. If multiple virtual machines access the same VMFS datastore and the same logical unit number (LUN), use disk shares to prioritize the disk accesses from the virtual machines. Disk shares distinguish high-priority from low-priority virtual machines.

You can allocate the host disk's I/O bandwidth to the virtual hard disks of a virtual machine. Disk I/O is a host-centric resource so you cannot pool it across a cluster.

Shares is a value that represents the relative metric for controlling disk bandwidth to all virtual machines. The values are compared to the sum of all shares of all virtual machines on the server.

Disk shares are relevant only within a given ESXi host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

You can select an IOP limit, which sets an upper bound for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab and select **Disk**.
- 3 In the Resource Allocation panel, select the virtual hard disk to change.
- 4 Click the **Shares** column and change the value to allocate a number of shares of its disk bandwidth to the virtual machine.
 - Low (500)
 - Normal (1000)
 - High (2000)
 - Custom

When you select a shares symbolic value, the numeric value appears in the **Shares Value** column. You can select **Custom** to enter a user-defined shares value.
- 5 Click the **Limit - IOPS** column and enter the upper limit of storage resources to allocate to the virtual machine.
- 6 Click **OK** to save your changes.

Converting Virtual Disks from Thin to Thick

You can determine whether your virtual disk is in the thin provision format and, if required, convert it to the thick provision format.

For more information on thin provisioning and available disk formats, see the *vSphere Storage* documentation.

Determine the Disk Format of a Virtual Machine in the vSphere Client

You can determine whether your virtual disk is in thick or thin format.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the appropriate hard disk in the Hardware list.

The Disk Provisioning section on the right shows the type of your virtual disk.
- 3 Click **OK**.

What to do next

If your virtual disk is in the thin format, you can inflate it to its full size.

Convert a Virtual Disk from Thin to Thick

If you created a virtual disk in the thin provision format, you can convert it to the thick provision format.

The thin provisioned disk starts small and at first, uses just as much storage space as it needs for its initial operations. After having been converted, the virtual disk grows to its full capacity and occupies the entire datastore space provisioned to it during the disk's creation.

Procedure

- 1 Select the virtual machine in the inventory.
- 2 Click the **Summary** tab and, under **Resources**, double-click the datastore for the virtual machine to open the Datastore Browser dialog box.
- 3 Click the virtual machine folder to find the virtual disk file you want to convert. The file has the .vmdk extension.
- 4 Right-click the virtual disk file and select **Inflate**.

The virtual disk in the thick provision format occupies the entire datastore space originally provisioned to it.

Virtual Machine Controller Configuration

To access virtual disks, SCSI, and CD/DVD-ROM devices, a virtual machine uses virtual controllers. You can add a controller or change the controller type. With SCSI controllers, you can select bus sharing for a virtual machine.

Virtual controllers appear to a virtual machine as different types of controllers, including BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, VMware Paravirtual SCSI, and SATA.

When you create a virtual machine, the default controller type depends on the guest operating system and device type and is optimized for best performance. For example, when you create virtual machines with Apple Mac OS X, the default controller type for both the hard disk and the CD/DVD drive is SATA. When you create virtual machines with Windows guests, a SCSI controller is the default for the hard disk and a SATA controller is the default for the CD/DVD drive.

Each virtual machine can have a maximum of eight controllers, including four SCSI controllers and four SATA controllers. The default controller is numbered as 0. When you create a virtual machine, the default hard disk is assigned to the default controller 0 at bus node (0:0).

When you add virtual controllers, they are numbered sequentially 1, 2, and 3. If you add a hard disk, SCSI, or CD/DVD-ROM device to a virtual machine after virtual machine creation, it is assigned to the first available virtual device node on the default controller, for example (0:1).

If you add a controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:z), where 1 is controller 1 and z is a virtual device node from 0 to 15.

By default, the virtual controller is assigned to virtual device node (z:7), so that device node is unavailable for hard disks or other devices.

Add SCSI Controllers

You can add SCSI controllers to an existing virtual machine by adding hard disks on unused SCSI Bus numbers.

Adding a new hard disk on an unused SCSI bus number automatically creates a new SCSI controller.

Prerequisites

Sufficient privileges to edit the virtual machine.

Procedure

- 1 Right-click on a virtual machine and select **Edit Settings**.
- 2 Select the Hardware tab.
- 3 Click **Add**.
- 4 Select **Hard Disk** and click **Next**.
- 5 Proceed through the wizard, selecting options that suit your needs.
- 6 In the Advanced Options page > Virtual Device Node section, select an unused SCSI Bus number.
For example, bus and device numbers 0:0 - 0:15 are used by the initial SCSI controller. The second SCSI controller uses bus and device numbers 1:0 - 1:15.
- 7 On the Ready to Complete page, click **Finish**.

The new hard disk and new SCSI controller are simultaneously created.

Change the SCSI Bus Sharing Configuration in the vSphere Client

You can set the type of SCSI bus sharing for a virtual machine and indicate whether the SCSI bus is shared. Depending on the type of sharing, virtual machines can access the same virtual disk simultaneously on the same server or on any server.

You can change the SCSI controller configuration for a virtual machine on an ESXi host only.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select a SCSI Controller in the hardware list.
- 3 Select the type of sharing in the **SCSI Bus Sharing** list.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Virtual	Virtual disks can be shared by virtual machines on the same server.
Physical	Virtual disks can be shared by virtual machines on any server.

- 4 Click **OK** to save your changes.

Change the SCSI Controller Type in the vSphere Client

You configure virtual SCSI controllers on your virtual machines to attach virtual disks and RDMs to.

The choice of SCSI controller does not affect whether your virtual disk is an IDE or SCSI disk. The IDE adapter is always ATAPI. The default for your guest operating system is already selected. Older guest operating systems default to the BusLogic adapter.

If you create an LSI Logic virtual machine and add a virtual disk that uses BusLogic adapters, the virtual machine boots from the BusLogic adapters disk. LSI Logic SAS is available only for virtual machines with hardware version 7 or later. Disks with snapshots might not experience performance gains when used on LSI Logic SAS, VMware Paravirtual, and LSI Logic Parallel adapters.



CAUTION Changing the SCSI controller type might result in a virtual machine boot failure.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab, select a SCSI controller, and click **Change Type**.
- 3 Select a SCSI controller type and click **OK**.
- 4 Click **OK** to save your changes.

About VMware Paravirtual SCSI Controllers

VMware Paravirtual SCSI controllers are high performance storage controllers that can result in greater throughput and lower CPU use. These controllers are best suited for high performance storage environments.

VMware Paravirtual SCSI controllers are available for virtual machines with ESXi 4.x and later compatibility. Disks on such controllers might not experience optimal performance gains if they have snapshots or if memory on the ESXi host is over committed. This behavior does not mitigate the overall performance gain of using VMware Paravirtual SCSI controllers as compared to other SCSI controller options.

If you have virtual machines with VMware Paravirtual SCSI controllers, those virtual machines cannot be part of an MSCS cluster.

For platform support for VMware Paravirtual SCSI controllers, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Add a Paravirtual SCSI Controller

You can add a VMware Paravirtual SCSI (PVSCSI) high performance storage controller to provide greater throughput and lower CPU utilization.

PVSCSI controllers are best suited for environments, especially SAN environments, running I/O-intensive applications.

Prerequisites

- Verify that the virtual machine has a guest operating system with VMware Tools installed.
- Verify that the virtual machine has hardware version 7 or later.
- Ensure that you are familiar with PVSCSI limitations. See [About VMware Paravirtual SCSI Controllers](#).
- To access boot disk devices attached to a PVSCSI controller, verify that the virtual machine has a Windows 2003 or Windows 2008 guest operating system.
- In some operating systems, before you change the controller type you need to create a virtual machine with an LSI Logic controller, install VMware Tools, then change to paravirtual mode.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select **SCSI Device** and click **Next**.

- 4 Select a SCSI device in the Connection panel.
- 5 Select an unused Virtual Device Node and click **Next**.
For device node SCSI (0:2), 0 is the controller number and 2 is the number of the device that is attached to the controller. If you select a node on which devices already exist (for example, SCSI 0:3) you will add a SCSI device to the existing controller. To add a new controller, you must select an unused device node on an unused SCSI controller (for example 1:0).
- 6 Review your selections and click **Finish**.
New SCSI Controller (adding) and **New SCSI Device (adding)** appear in the Hardware list.
- 7 Click **OK** to save your changes and exit the dialog box.
- 8 Reopen the Virtual Machine Properties Editor.
- 9 Select the new SCSI controller and click **Change Type**.
- 10 Select **VMware Paravirtual** and click **OK**.
- 11 Click **OK** to save your changes.

Other Virtual Machine Device Configuration

In addition to configuring virtual machine CPU and Memory and adding a hard disk and virtual NICs, you can also add and configure virtual hardware, such as DVD/CD-ROM drives, floppy drives, and SCSI devices. Not all devices are available to add and configure. For example, you cannot add a video card, but you can configure available video cards and PCI devices.

Change the CD/DVD Drive Configuration

You can configure DVD or CD devices to connect to client devices, host devices, or Datastore ISO files.

Configure a Client Device Type for the DVD/CD-ROM Drive in the vSphere Client

You can connect the DVD/CD-ROM device to a physical DVD or CD-ROM device on the system running the vSphere Client.

Procedure

- 1 Select the virtual machine in the vSphere Client inventory.
- 2 Click the **CD/DVD Connections** icon on the virtual machine toolbar.
- 3 Select a drive or ISO image from the **CD/DVD drive** drop-down menu.

Passthrough IDE (raw) mode access is set by default, which lets you write or burn a remote CD.

Configure a Host Device Type for the DVD/CD-ROM Drive in the vSphere Client

You can connect the DVD/CD-ROM device to a physical DVD or CD-ROM device that resides on the host.

You cannot use vMotion to migrate virtual machines that have CD drives that are backed by the physical CD drive on the host. You must disconnect these devices before you migrate the virtual machine.

When you add a CD/DVD-ROM drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding or removing SCSI devices from an ESXi host is not supported.

Prerequisites

Ensure that the host is powered off before you add USB CD/DVD-ROM devices.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the DVD/CD-ROM drive.
- 3 Select or deselect the **Connected** check box to connect or disconnect the device.
- 4 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.
- 5 Select **Host Device** under **Device Type** and select a device from the drop-down menu.
- 6 (Optional) In the drop-down menu under **Virtual Device Node**, select the node the drive uses in the virtual machine.
- 7 Click **OK** to save your changes.

Configure a Datastore ISO File for the DVD/CD-ROM Drive in the vSphere Client

You can connect the DVD/CD-ROM device to an ISO file that is stored on a datastore accessible to the host.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the DVD/CD-ROM drive.
- 3 Select or deselect the **Connected** check box to connect or disconnect the device.
- 4 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.
- 5 Select **Datastore ISO File** under **Device Type** and click **Browse** to navigate to the file.
- 6 In the drop-down menu under **Virtual Device Node**, select the node the drive uses in the virtual machine.
- 7 Click **OK** to save your changes.

Add a DVD or CD-ROM Drive to a Virtual Machine in the vSphere Client

You can use a physical drive on a client or host or you can use an ISO image to add a DVD/CD-ROM drive to a virtual machine.

If you are adding a CD/DVD-ROM drive that is backed by USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding or removing SCSI devices from an ESXi host is not supported.

You cannot use vMotion to migrate virtual machines that have CD drives that are backed by the physical CD drive on the host. You must disconnect these devices before you migrate the virtual machine.

Prerequisites

Ensure that the host is powered off before you add USB DVD/CD-ROM devices.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Select the **Hardware** tab and click **Add**.
- 3 Select **DVD/CD-ROM Drive**, and click **Next**.

- 4 Select one option.

Option	Description
Use physical drive	<ol style="list-style-type: none"> a Select Client or Host as the location. b Select the drive you want to use from the drop-down menu. c Select a Pass through (recommended) or ATAPI emulation connection type.
Use ISO Image	Enter the path and filename for the image file, or click Browse to navigate to the file.

- 5 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.
- 6 Click **Next**.
- 7 Select the virtual device node the drive uses in the virtual machine and click **Next**.
- 8 Review the information on the **Ready to Complete** window, and click **Finish** or click **Back** to change the settings.
- 9 Click **OK** to save your changes.

Change the Floppy Drive Configuration in the vSphere Client

You can configure a virtual floppy drive device to connect to a client device or to an existing or new floppy image.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

NOTE You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4. 0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select the Floppy drive.
- 3 Under Device Status, select **Connect at power on** to connect this virtual machine to the floppy drive when the virtual machine is powered on.
- 4 Select the device type to use for this virtual device.

Option	Description
Client Device	<p>Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system running the vSphere Client.</p> <p>To connect the device, click the Floppy Connections button in the toolbar when you power on the virtual machine.</p>
Use existing floppy image in datastore	<ol style="list-style-type: none"> a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click Browse and select the floppy image.
Create new floppy image in datastore	<ol style="list-style-type: none"> a Select this option to create a floppy image on a datastore accessible to the host. b Click Browse and browse to the location for the floppy image. c Enter a name for the floppy image and click OK.

- 5 Click **OK** to save your changes.

Add a Floppy Drive to a Virtual Machine in the vSphere Client

Use a physical floppy drive or a floppy image to add a floppy drive to a virtual machine.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

NOTE You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4.0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Select the **Hardware** tab and click **Add**.
- 3 Select **Floppy Drive**, and click **Next**.
- 4 Select the device type to use for this virtual device.

Option	Description
Use a physical floppy drive	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system running the vSphere Client. To connect the device, click the Floppy Connections button in the toolbar when you power on the virtual machine.
Use a floppy image	<ol style="list-style-type: none"> a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click Browse and select the floppy image.
Create a blank floppy image	<ol style="list-style-type: none"> a Select this option to create a floppy image on a datastore accessible to the host. b Click Browse and browse to the location for the floppy image. c Enter a name for the floppy image and click OK.

- 5 To have the floppy drive connected to the virtual machine when you power it on, select **Connect at power on**.
- 6 Click **Next**.
- 7 Review the information on the Ready to Complete page, and click **Finish**.
- 8 Click **OK** to save your changes.

Add a SCSI Device to a Virtual Machine in the vSphere Client

You can add a SCSI device to a virtual machine through the Add Hardware wizard.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **Add**.
- 3 Select **SCSI Device** and click **Next**.
- 4 Under **Connection**, use the drop-down menu to select a physical device.
- 5 Under **Virtual Device Node**, select the virtual device node where you want this device to appear in the virtual machine.
- 6 Review the information in the Ready to Complete page, and click **Finish**.
- 7 Click **OK** to save your changes.

Change the SCSI Device Configuration in the vSphere Client

You can change the physical device and the virtual device node of the SCSI device connection.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select a SCSI device in the Hardware list.
- 3 Under **Connection**, select the physical device you want to use.
Under Virtual device node, select the virtual device node where you want this device to appear in the virtual machine.
- 4 Click **OK** to save your changes.

Add a PCI Device in the vSphere Client

vSphere DirectPath I/O allows a guest operating system on a virtual machine to directly access physical PCI and PCIe devices connected to a host. Each virtual machine can be connected to up to six PCI devices.

PCI devices connected to a host can be marked as available for passthrough from the Hardware Advanced Settings in the **Configuration** tab for the host.

Snapshots are not supported with PCI vSphere Direct Path I/O devices.

Prerequisites

- To use DirectPath I/O, verify that the host has Intel[®] Virtualization Technology for Directed I/O (VT-d) or AMD I/O Virtualization Technology (IOMMU) enabled in the BIOS.
- Verify that the PCI devices are connected to the host and marked as available for passthrough.
- Verify that the virtual machine is using hardware version 7 or later.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 On the **Hardware** tab, click **Add**.
- 3 In the Add Hardware wizard, select **PCI Device** and click **Next**.
- 4 Select the passthrough device to connect to the virtual machine from the drop-down list and click **Next**.
- 5 Click **Finish**.

Configure the Virtual Machine Communication Interface in the vSphere Client

The Virtual Machine Communication Interface (VMCI) provides a high-speed communication channel between a virtual machine and the ESXi host that it runs on. You can also enable VMCI for communication between virtual machines that run on the same host.

This setting applies to ESXi 5.0 and earlier virtual machines. It does not apply to ESXi 5.1 and later virtual machines. In vSphere 5.1, vSphere 5.5, and later, the `vmci0.unrestricted` setting has no effect, because guest-to-guest VMCI communication has been permanently disabled.

If VMCI is not restricted, a virtual machine can detect and be detected by all others with the same option enabled within the same host. Custom-built software that uses this interface might have unexpected vulnerabilities that lead to an exploit. Also, a virtual machine could detect how many other virtual machines are within the same ESX/ESXi system by registering the virtual machine. This information could be used for a malicious objective. The virtual machine can be exposed to others within the system as long as at least one program is connected to the VMCI socket interface. Use the following `.vmx` setting to restrict VMCI:

```
vmci0.unrestricted = "FALSE"
```

Prerequisites

Verify that the virtual machine is using hardware version 7 or later.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 On the **Hardware** Tab, select **Show All Devices** and click **VMCI device**.
- 3 Select the **Enable VMCI Between VMs** check box.
- 4 Click **OK** to save your changes.

Virtual machine communication is no longer restricted to the host it runs on. Other virtual machines that run on the same host can now communicate with the unrestricted virtual machine.

Configure Video Cards in the vSphere Client

You can change the number of displays for a virtual machine, allocate memory for the displays, and enable 3D support.

The default setting for total video RAM is adequate for minimal desktop resolution. For more complex situations, you can change the default memory.

Some 3D applications require a minimum video memory of 64MB. Keep this in mind when you assign video memory.

Prerequisites

Verify that the virtual machine is powered off.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **Video card**.
- 3 Select the display settings type and configure the available settings.

Option	Description
Auto-detect video settings	Applies common video settings to the guest operating system.
Specify custom settings	Lets you select the number of displays and the total video memory.

- 4 Select the number of displays from the drop-down menu.

The vSphere Client supports setting a number of displays and extending the screen across them. True multimonitor support is not available with the vSphere Client.

- 5 Enter the video memory required for the displays.
- 6 (Optional) Click **Video Memory Calculator** to calculate the required video memory based on the maximum number of displays, resolution, and color depth that the guest operating system must support and click **OK**.

- 7 (Optional) Click **Enable 3D support**.

This check box is active only for guest operating systems on which VMware supports 3D.

- 8 Click **OK** to save your changes.

Sufficient memory allocation is set for the virtual machine's video display.

USB Configuration from an ESXi Host to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices are connected to an ESXi host. USB passthrough technology supports adding USB devices, such as security dongles and mass storage devices to virtual machines that reside on the host to which the devices are connected.

How USB Device Passthrough Technology Works

When you attach a USB device to a physical host, the device is available only to virtual machines that reside on that host. The device cannot connect to virtual machines that reside on another host in the datacenter.

A USB device is available to only one virtual machine at a time. When a device is connected to a powered-on virtual machine, it is not available to connect to other virtual machines that run on the host. When you remove the active connection of a USB device from a virtual machine, it becomes available to connect to other virtual machines that run on the host.

Connecting a USB passthrough device to a virtual machine that runs on the ESXi host to which the device is physically attached requires an arbitrator, a controller, and a physical USB device or device hub.

USB Arbitrator

Manages connection requests and routes USB device traffic. The arbitrator is installed and enabled by default on ESXi hosts. It scans the host for USB devices and manages device connection among virtual machines that reside on the host. It routes device traffic to the correct virtual machine instance for delivery to the guest operating system. The arbitrator monitors the USB device and prevents other virtual machines from using it until you release it from the virtual machine it is connected to.

USB Controller

The USB hardware chip that provides USB function to the USB ports that it manages. The virtual USB Controller is the software virtualization of the USB host controller function in the virtual machine.

USB controller hardware and modules that support USB 2.0 and USB 1.1 devices must exist on the host. Two virtual USB controllers are available to each virtual machine. A controller must be present before you can add USB devices to the virtual computer.

The USB arbitrator can monitor a maximum of 15 USB controllers. Devices connected to controllers numbered 16 or greater are not available to the virtual machine.

USB Devices

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine. The maximum number of USB devices supported on a single ESXi host for simultaneous connection to one or more virtual machines is also 20. For a list of supported USB devices, see the VMware knowledge base article at <http://kb.vmware.com/kb/1021345>.

Connecting USB Devices to an ESXi Host

You can connect and chain multiple USB hubs and devices to an ESXi host. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the host. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the host does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the host USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Communication delay between the host and virtual machine increases as the number of cascading hubs increases.
- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.
- Chaining hubs together also increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the host rather than to a hub or extension cable might resolve their connection or performance issues.

NOTE To prevent additional problems, be aware of the physical constraints of long-term deployment in a machine room environment. Small devices are easily damaged by being stepped on or knocked loose.

In some cases, you must hard reset the device and hub to restore the device to a working state.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see the VMware knowledge base article at <http://kb.vmware.com/kb/1021345>.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Connect USB Devices to an ESXi Host

You can connect multiple USB devices to ESXi hosts so that virtual machines that run on the hosts can access the devices. The number of devices that you can connect depends on several factors, such as how the devices and hubs chain together and the device type.

Each ESXi host has several USB ports. The number of ports on each host depends on the physical setup of the host. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

The host treats USB CD/DVD-ROM devices as SCSI devices. Hot adding and removing these devices is not supported.

Prerequisites

- If a host has attached USB devices and resides in a DRS cluster with DPM enabled, disable DPM for that host. See the *vSphere Resource Management* documentation for instructions about overriding the default DPM setting for an individual host.
- Verify that you know the virtual machine requirements for USB devices. See [Connecting USB Devices to an ESXi Host](#).
- Verify that the ESXi host is powered off before you add USB CD/DVD-ROM devices.

Procedure

- ◆ To add a USB device to an ESXi host, connect the device to an available port or hub.

The USB device appears in the virtual machine Add Hardware wizard device list.

What to do next

You can now add the device to the virtual machine.

Add a USB Controller to a Virtual Machine in the vSphere Client

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or client computer to the virtual machine.

You can add two USB controllers to a virtual machine. The xHCI controller, available for Linux, Windows 8 and later, and Windows Server 2012 and later guest operating systems, supports USB 3.0 superspeed, 2.0, and 1.1 devices. The EHCI+UHCI controller supports USB 2.0 and 1.1 devices.

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 10-3. USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to VM	Supported for Passthrough from Client Computer to VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.0, 2.0, and 1.1	Yes (USB 2.0 and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

NOTE Drivers are not available for the xHCI controller on Windows guest operating systems.

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 2.0 and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select the type of **USB Controller** to add and click **Next**.
- 4 Review the device information and click **Next**.
- 5 Click **Finish**.

New USB Controller (adding) appears in the hardware list as **Present**.

- 6 Click **OK** to save your changes.

When you reopen the Properties Editor, the xHCI controller appears on the **Hardware** tab as USB xHCI controller. The EHCI+UHCI controller appears as **USB controller**.

What to do next

Add one or more USB devices to the virtual machine.

Add USB Devices from an ESXi Host to a Virtual Machine in the vSphere Client

You can add one or more USB passthrough devices from an ESXi host to a virtual machine if the physical device is connected to the host on which the virtual machine runs.

If a USB device is connected to another virtual machine, you cannot add it until that machine releases it.

NOTE If you have the Apple Frontpanel Controller device in your environment, you can safely add it to a virtual machine. However, this device has no documented function and no known use. ESXi hosts do not use it and do not provide Xserver functionality for USB passthrough

Prerequisites

- Verify that the virtual machine is using hardware version 7 or later.
- Verify that a USB controller is present. See [“Add a USB Controller to a Virtual Machine in the vSphere Client,”](#) on page 97.
- To use vMotion to migrate a virtual machine with multiple USB devices, you must enable all attached USB devices for vMotion. You cannot migrate individual USB devices.
- When you add a CD/DVD-ROM drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.
- Verify that you know the virtual machine requirements for USB devices. See [USB Configuration from an ESXi Host to a Virtual Machine](#).
- Required privileges: **Virtual Machine.Configuration.HostUSBDevice**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select **USB Device** and click **Next**.
- 4 (Optional) Select **Support vMotion while device is connected**.
- 5 If you do not plan to migrate a virtual machine with USB devices attached, deselect the **Support vMotion** option.

This reduces migration complexity, which results in better performance and stability.

- 6 Select a device to add.
You can add multiple USB devices, but only one device at a time.
- 7 Click **Finish**.
New USB Device (adding) appears in the hardware list as **Present**.
- 8 Click **OK** to save your changes.

When you reopen the Properties editor, the USB device appears on the **Hardware** tab of the Properties Editor. The device type and ID appear in the right pane.

Remove a USB Device from a Virtual Machine

When you remove a USB device from a virtual machine, it reverts to the host and becomes available to other virtual machines that run on that host.

To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a "Remove Hardware" icon located in the System Tray. Linux operating systems use the **umount** command.

NOTE It might be necessary to use the **sync** command instead of or in addition to the **umount** command, for example after you issue a **dd** command on Linux or other UNIX operating systems.

Procedure

- 1 Unmount or eject the USB device from the guest operating system.
- 2 Right-click the virtual machine and select **Edit Settings**.
- 3 Click the **Hardware** tab and select the USB device.
- 4 Click **Remove** and click **OK** to save your changes and close the dialog box.

Remove a USB Controller from a Virtual Machine in the vSphere Client

You can remove a USB controller from a virtual machine if you do not want to connect to USB devices.

Prerequisites

- Verify that all USB devices are disconnected from the virtual machine.
- Required Privilege: **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **USB controller**.

- 3 Click **Remove**.
- 4 Click **OK** to save your changes.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Remove USB Devices from an ESXi Host

You can remove USB devices from the host if you must shut down the host for maintenance or if you do not want those devices to be available to virtual machines that run on the host. When you detach a USB device from the host, the device disconnects from the virtual machine.



CAUTION If data transfer is taking place when you remove USB devices from a host, you can lose data.

Prerequisites

Verify that the USB devices are not in use.

Procedure

- ◆ Follow the device manufacturers instructions to safely remove the device.

When you remove the device from the host, it is no longer available to the virtual machines that run on the host.

USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client

You can add multiple USB devices to a virtual machine when the physical devices connect to a client computer on which the vSphere Client is running. The vSphere Client must be logged in to an instance of vCenter Server that manages the ESXi host or directly into the host where the virtual machines reside. USB passthrough technology supports adding multiple USB devices, such as security dongles, mass storage devices, and smartcard readers to virtual machines.

How USB Device Passthrough Technology Works

The USB controller is the USB hardware chip that provides USB function to the USB ports that it manages. USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist in the virtual machine. Two USB controllers are available for each virtual machine. The controllers support multiple USB 3.0, 2.0, and 1.1 devices. The controller must be present before you can add USB devices to the virtual machine.

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine.

You can add multiple devices to a virtual machine, but only one at a time. The virtual machine retains its connection to the device while in S1 standby. USB device connections are preserved when you migrate virtual machines to another host in the datacenter.

A USB device is available to only one powered-on virtual machine at a time. When a virtual machine connects to a device, that device is no longer available to other virtual machines or to the client computer. When you disconnect the device from the virtual machine or shut the virtual machine down, the device returns to the client computer and becomes available to other virtual machines that the client computer manages.

For example, when you connect a USB mass storage device to a virtual machine, it is removed from the client computer and does not appear as a drive with a removable device. When you disconnect the device from the virtual machine, it reconnects to the client computer's operating system and is listed as a removable device.

USB 3.0 Device Limitations

USB 3.0 devices have the following requirements and limitations:

- The virtual machine that you connect the USB 3.0 device to must be configured with an xHCI controller and have a Linux guest operating system with a 2.6.35 or later kernel.
- You can connect only one USB 3.0 device operating at superspeed to a virtual machine at a time.
- USB 3.0 devices are available only for passthrough from a client computer to a virtual machine. They are not available for passthrough from an ESXi host to a virtual machine.

Avoiding Data Loss

Before you connect a device to a virtual machine, make sure the device is not in use on the client computer.

If the vSphere Client disconnects from the vCenter Server or host, or if you restart or shut down the client computer, the device connection breaks. It is best to have a dedicated client computer for USB device use or to reserve USB devices connected to a client computer for short-term use, such as updating software or adding patches to virtual machines. To maintain USB device connections to a virtual machine for an extended time, use USB passthrough from an ESXi host to the virtual machine.

vSphere Features Available with USB Passthrough from a Client Computer

Migration with vMotion, DRS, and DPM are supported with USB device passthrough from a client computer to a virtual machine.

Table 10-4. Features Available for USB Passthrough from a Remote Computer to a Virtual Machine

Feature	Supported with USB Device Passthrough
vSphere Distributed Power Management (DPM)	Yes
vSphere Distributed Resource Scheduler (DRS)	Yes
vSphere HA	No
vSphere Fault Tolerance	No
vSphere vMotion	Yes

Connecting USB Devices to a Client Computer

You can connect and chain any multiple low, full, and high- or super-speed USB hubs and devices to a client computer. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the client computer. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the client computer does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the client computer USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.

- Chaining hubs together increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the client computer rather than to a hub or extension cable might resolve their connection or performance issues. In some cases, you must remove and reattach the device and hub to restore the device to a working state.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Connect USB Devices to a Client Computer

You can connect multiple USB devices to a client computer so that virtual machines can access the devices. The number of devices that you can add depends on several factors, such as how the devices and hubs chain together and the device type.

The number of ports on each client computer depends on the physical setup of the client. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

Verify that you know the requirements for configuring USB devices from a remote computer to a virtual machine.

Procedure

- ◆ To add a USB device to a client computer, connect the device to an available port or hub.

The USB device appears in the virtual machine toolbar menu.

What to do next

You can now add the USB device to the virtual machine.

Add a USB Controller to a Virtual Machine in the vSphere Client

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or client computer to the virtual machine.

You can add two USB controllers to a virtual machine. The xHCI controller, available for Linux, Windows 8 and later, and Windows Server 2012 and later guest operating systems, supports USB 3.0 superspeed, 2.0, and 1.1 devices. The EHCI+UHCI controller supports USB 2.0 and 1.1 devices.

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 10-5. USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to VM	Supported for Passthrough from Client Computer to VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.0, 2.0, and 1.1	Yes (USB 2.0 and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

NOTE Drivers are not available for the xHCI controller on Windows guest operating systems.

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 2.0 and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and click **Add**.
- 3 Select the type of **USB Controller** to add and click **Next**.
- 4 Review the device information and click **Next**.
- 5 Click **Finish**.

New USB Controller (adding) appears in the hardware list as **Present**.

- 6 Click **OK** to save your changes.

When you reopen the Properties Editor, the xHCI controller appears on the **Hardware** tab as USB xHCI controller. The EHCI+UHCI controller appears as **USB controller**.

What to do next

Add one or more USB devices to the virtual machine.

Add USB Devices From a Client Computer to a Virtual Machine in the vSphere Client

You can add one or more USB passthrough devices from a client computer to a virtual machine in the vSphere Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machines reside.

The devices maintain their virtual machine connections in S1 standby, if the vSphere Client is running and connected. After you add the USB device to the virtual machine, an information message appears on the client computer stating that the device is disconnected. The device remains disconnected from the client computer until the virtual machine releases it.

FT is not supported with USB passthrough from a client computer to a virtual machine.

Prerequisites

- Verify that a USB controller is installed.
- Verify that the vSphere Client is connected to the ESXi host on which the virtual machines are running.
- Required Privilege: **Virtual Machine.Interaction.Add or Remove Device**

Procedure

- 1 Select the virtual machine in the vSphere Client inventory.
- 2 Click the USB icon on the virtual machine toolbar.
- 3 Select an available device from the **Connect to USB Devices** drop-down menu.

The status of the device appears as Connecting.

The device appears in the **USB Connections** drop-down menu and is ready to use. The device remains connected until you power off the virtual machine or disconnect the vSphere Client from the ESXi host.

Remove USB Devices That Are Connected Through a Client Computer in the vSphere Client

You can remove USB devices from a virtual machine if the devices are no longer needed. When you disconnect a USB device from a virtual machine, the device is released from the virtual machine and is given back to the client computer, which starts using it.

Prerequisites

To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a "Remove Hardware" icon located in the System Tray. Linux operating systems use the **umount** command.

NOTE You might need to use the sync command instead of or in addition to the umount command, for example after you run a dd command on Linux or other UNIX operating systems.

Procedure

- 1 Unmount or eject the USB device from the guest operating system.
- 2 Select the virtual machine in the vSphere Client inventory.
- 3 Click **USB Connections** on the virtual machine toolbar.

- 4 Select the device to remove from the drop-down menu.

For example, select **USB Device 1** > **Disconnect from *device name***.

The menu shows the device status as Disconnecting.

The device reconnects to the client computer and is available to add to another virtual machine. In some cases, Windows Explorer detects the device and opens a dialog box on the client computer. You can close this dialog box.

Remove a USB Controller from a Virtual Machine in the vSphere Client

You can remove a USB controller from a virtual machine if you do not want to connect to USB devices.

Prerequisites

- Verify that all USB devices are disconnected from the virtual machine.
- Required Privilege: **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Hardware** tab and select **USB controller**.
- 3 Click **Remove**.
- 4 Click **OK** to save your changes.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Remove USB Devices from a Client Computer

You can remove USB devices from a client computer if you do not want those devices to be available to virtual machines.

When you detach a USB device from the remote client, the device disconnects from the virtual machine. Ensure that data transfer is not taking place before you remove the device.

Prerequisites

Verify that the devices are not in use.

Procedure

- ◆ To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the **umount** command.

You might need to use the `sync` command instead of or in addition to the `umount` command, for example after you issue a `dd` command on Linux or other UNIX operating systems.

When you remove the device from the client computer, it is no longer available to virtual machines.

Add a Shared Smart Card Reader to Virtual Machines in the vSphere Client

You can configure multiple virtual machines to use a virtual shared smart card reader for smart card authentication. The smart card reader must be connected to a client computer on which the vSphere Client runs. All smart card readers are treated as USB devices.

A license is required for the shared smart card feature. See the *vCenter Server and Host Management* documentation.

When you log out of Windows XP guest operating systems, to log back in, you must remove the smart card from the smart card reader and re-add it. You can also disconnect the shared smart card reader and reconnect it.

If the vSphere Client disconnects from the vCenter Server or host, or if the client computer is restarted or shut down, the smart card connection breaks. For this reason, it is best to have a dedicated client computer for smart card use.

To connect a USB smart card reader that is not shared, see [“USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client,”](#) on page 100.

Prerequisites

- Verify that the smart card reader is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.

Procedure

- 1 Select the virtual machine in the vSphere Client inventory.
- 2 Click the USB icon on the virtual machine toolbar.
- 3 Select the shared smart card reader from the **Connect to USB Devices** drop-down menu.
The smart card device appears in the menu as a USB device and as a virtual shared device.
- 4 Select **Shared** *the model name of your smart card reader* followed by a number.
The device status appears as Connecting, then the device connects.

You can now use smart card authentication to log in to virtual machines in the vSphere Client inventory.

Manage Power Management Settings for a Virtual Machine

You can set the power options so that a virtual machine is suspended or remains powered on when the guest operating system is placed on standby.

Power Management options are not available on every guest operating system. **Wake on LAN** supports only Windows guest operating systems and is not available on Vlan NICs, or when a Flexible NIC is operating in Vlan mode (that is, the current VMware Tools are not installed on the guest operating system).

Wake on LAN can resume virtual machines that are in an S1 sleep state only. It cannot resume suspended, hibernated, or powered off virtual machines.

The following NICs support **Wake on LAN**:

- Flexible (VMware Tools required).
- vmxnet

- Enhanced vmxnet
- vmxnet 3

Prerequisites

You must power off the virtual machine.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **Power Management**.
- 3 In the **Guest Power Management** panel, select a power option.
 - **Suspend the virtual machine**
 - **Put the guest operating system in standby mode and leave the virtual machine powered on**
- 4 (Optional) Select **Wake on LAN for virtual machine traffic on** and select the virtual NICs to trigger this action.
 Unsupported NICs might be listed, but are unavailable to connect.
- 5 Click **OK** to save your changes.





Configure the Virtual Machine Power States

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the toolbar power controls or you can configure the controls to interact with the guest operating system. For example, you can configure the stop button on the toolbar to power off the virtual machine or shut down the guest operating system.

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

[Table 10-6](#) lists available power buttons and describes their behavior.

Table 10-6. Virtual Machine Power Button Settings

Power Button	Description
	Shuts down the guest operating system or powers off the virtual machine. A power off operation displays a confirmation dialog box indicating that the guest operating system might not shut down properly. Use this power off option only when necessary.
	Suspends the virtual machine without running a script when VMware Tools is not installed. When VMware Tools is installed and available, a suspend action runs a script, and suspends the virtual machine.
	Powers on a virtual machine when a virtual machine is stopped, or resumes the virtual machine and runs a script when it is suspended and VMware Tools is installed and available. Resumes the virtual machine and does not run a script when VMware Tools is not installed.
	Resets the virtual machine when VMware Tools is not installed. Restarts the guest operating system when VMware Tools is installed and available. A reset operation displays a confirmation dialog box indicating that the guest operating system is not shut down properly.

Prerequisites

- Verify that you have access to at least one virtual machine in the inventory.
- Verify that you have privileges to perform the intended power operation on the virtual machine.

- To set optional power functions, you must install VMWare Tools in the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **VMware Tools**.
- 3 In the right panel, select the **Power Controls** for the virtual machine.
- 4 Select an option for the **Power Off** button.

Option	Description
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. This type of powering off is known as a "soft" power operation. Soft power operations are possible only if the tools are installed in the guest operating system.
Power Off	Immediately stops the virtual machine. This type of powering off is known as a "hard" power operation.
System Default	Follows system settings. The current value of the system settings is shown in parentheses.

- 5 Select an option for the **Suspend** button.

Option	Description
Suspend	Pauses all virtual machine activity.
System Default	Follows system settings. The current value of the system setting is shown in parentheses.

- 6 Select an option for the **Reset** button.

Option	Description
Restart Guest	Uses VMware Tools to initiate an orderly reboot. (This type of reset is known as a "soft" power operation. Soft power operations are possible only if the tools are installed in the guest operating system.)
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. (This type of reset is known as a "hard" power operation.)
System Default	Follows system settings; the current value of the system setting is shown in parentheses.

- 7 Click **OK** to save your changes.

What to do next

Configure VMware Tools scripts to run before or after power operations.

Delay the Boot Sequence in the vSphere Client

The time between when you power on the virtual machine and when it exits the BIOS or EFI and launches the guest operating system software can be short. You can change the boot delay or force the virtual machine to enter the BIOS or EFI setup screen after power on.

Delaying the boot operation is useful for changing BIOS or EFI settings such as the boot order. For example, you can change the BIOS or EFI settings to force a virtual machine to boot from a CD-ROM.

Prerequisites

Required Privilege: **Virtual machine.Configuration.Settings**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and under Advanced select **Boot Options**.
- 3 In the **Power on Boot Delay** panel, select the time in milliseconds to delay the boot operation.
- 4 (Optional) Select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.
- 5 (Optional) Select whether to try to reboot after a boot failure.
- 6 Click **OK** to save your changes.

Enable Logging in the vSphere Client

You can enable logging to collect log files to help troubleshoot issues with your virtual machine.

Required privilege: **Virtual machine.Configuration.Settings**

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Options** tab and select **AdvancedGeneral**.
- 3 In the **Settings** pane, select **Enable logging**.
- 4 Click **OK**.

Disable Acceleration in the vSphere Client

You can temporarily disable acceleration to allow a virtual machine to successfully run or install software.

In rare instances, you might find that when you install or run software in a virtual machine, the virtual machine appears to stop responding. Generally, the problem occurs early in the program's execution. Often, you can get past the problem by temporarily disabling acceleration in the virtual machine.

This setting slows down virtual machine performance, so only use it for getting past the problem with running the program. After the program stops encountering problems, deselect **Disable acceleration**. Then you might be able to run the program with acceleration.

You can enable and disable acceleration when the virtual machine is running.

Procedure

- 1 Click the **Options** tab.
- 2 Select **Advanced > General** in the **Settings** list.
- 3 To disable acceleration, select the **Disable acceleration** check box.

Configure Debugging and Statistics in the vSphere Client

You can run a virtual machine so that it collects debugging information and statistics that are helpful to VMware technical support in resolving issues.

Procedure

- 1 Click the **Options** tab and click **Advanced > General**.

- 2 To enable debugging mode, select an option from the **Debugging and Statistics** section.

Option	Description
Run normally	Collects debugging information.
Record debugging information	Collects debugging and performance information. Use this option to aid troubleshooting when the guest operating system crashes or is not behaving properly.

Managing Virtual Machines

When you connect directly to a host using the vSphere Client, you can open a console to any of the host's virtual machines, add and remove virtual machines in the host's inventory, and manage virtual machine snapshots.

This chapter includes the following topics:

- [“Edit Virtual Machine Startup and Shutdown Settings,”](#) on page 111
- [“Open a Console to a Virtual Machine,”](#) on page 112
- [“Remove Virtual Machines from a Host,”](#) on page 112
- [“Remove Virtual Machines from the Datastore,”](#) on page 113
- [“Return a Virtual Machine or Template to a Host,”](#) on page 113
- [“Using Snapshots To Manage Virtual Machines,”](#) on page 113

Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host. You can also set the default timing and startup order for selected virtual machines. This ability allows the operating system to save data when the host enters maintenance mode or is being powered off for another reason.

The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

Procedure

- 1 In the vSphere Client inventory, select the host where the virtual machine is located and click the **Configuration** tab.
- 2 Under Software, click **Virtual Machine Startup/Shutdown** and click **Properties**.
The Virtual Machine Startup and Shutdown dialog box opens.
- 3 Select **Allow virtual machines to start and stop automatically with the system**.

- 4 (Optional) Configure the startup and shutdown behavior.

Option	Action
Default Startup Delay	Select the amount of time to delay starting the operating system. This delay allows time for VMware Tools or the booting system to run scripts.
Continue immediately if the VMware Tools starts	Select to start the operating system immediately after VMware Tools starts.
Default Shutdown Delay	Select the amount of time to delay shutdown for each virtual machine. The shutdown delay applies only if the virtual machine does not shut down before the delay period elapses. If the virtual machine shuts down before the delay time is reached, the next virtual machine starts shutting down.
Shutdown Action	Select a shutdown option from the drop-down menu. <ul style="list-style-type: none"> ■ Power Off ■ Suspend ■ Guest Shutdown
Move Up and Move Down	Select a virtual machine in the Manual Startup category and use the Move Up button to move it up to Automatic Startup or Any Order. When virtual machines are in the Automatic Startup category, you can use Move Up and Move Down to order them so that they start in a preferred sequence. During shutdown, the virtual machines are stopped in the opposite order.
Edit	Click Edit to configure user-specified autostartup and shutdown behavior for virtual machines in the Automatic Startup or Any Order category.

- 5 Click **OK** to close the dialog box and save your settings.

Open a Console to a Virtual Machine

With the vSphere Client, you can access a virtual machine's desktop by launching a console to the virtual machine. From the console, you can perform activities within the virtual machine such as configure operating system settings, run applications, monitor performance, and so on.

Procedure

- 1 In the vSphere Client inventory, right-click the virtual machine and select **Open Console**.
- 2 Click anywhere inside the console window to enable your mouse, keyboard, and other input devices to work in the console.

Remove Virtual Machines from a Host

Removing a virtual machine from the inventory unregisters it from the host, but does not delete it from the datastore. Virtual machine files remain at the same storage location and the virtual machine can be re-registered by using the datastore browser.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Display the virtual machine in the inventory.
- 2 Right-click the virtual machine and select **Remove from Inventory**.
- 3 To confirm that you want to remove the virtual machine from the inventory, click **OK**.

The host removes references to the virtual machine and no longer tracks its condition.

Remove Virtual Machines from the Datastore

You use the **Delete from Disk** option to remove a virtual machine from a host and delete all virtual machine files, including the configuration file and virtual disk files, from the datastore.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Display the virtual machine in the inventory.
- 2 Right-click the virtual machine and select **Delete from Disk**.
- 3 Click **OK** in the confirmation dialog box.

The host deletes the virtual machine from its datastore. Disks that are shared with other virtual machines are not deleted.

Return a Virtual Machine or Template to a Host

If you remove a virtual machine or template from a host, but do not remove it from the host's datastore, you can return it to the host's inventory by using the Datastore Browser.

Procedure

- 1 Display the datastore in the inventory.
- 2 Right-click the datastore and select **Browse Datastore**.
- 3 Navigate to the virtual machine or template to add to the inventory.
- 4 Right-click the virtual machine or template and select **Add to Inventory**.
- 5 Complete the Add to Inventory wizard to add the virtual machine or template.

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking snapshots for all members of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before diverging a virtual machine in the snapshot tree.

The Snapshot Manager in the vSphere Web Client and the vSphere Client provide several operations for creating and managing virtual machine snapshots and snapshot trees. These operations let you create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create extensive snapshot trees that you can use to save the virtual machine state at any specific time and restore the virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes disks that were added or changed after you took the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The Snapshot Manager presents the snapshot hierarchy as a tree with one or more branches. The relationship between snapshots is like that of a parent to a child. In the linear process, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshots. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or restore any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you restore a snapshot and take another snapshot, a branch, or child snapshot, is created.

Parent Snapshots

The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base .vmdk file. The parent snapshot is always the snapshot that appears immediately above the You are here icon in the Snapshot Manager. If you revert or restore a snapshot, that snapshot becomes the parent of the You are here current state.

NOTE The parent snapshot is not always the snapshot that you took most recently.

Child Snapshots

A snapshot that is taken of the same virtual machine after the parent snapshot. Each child constitutes delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

IMPORTANT Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk using `vmkfstools`.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta .vmdk disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base .vmdk file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Taking Snapshots

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Memory snapshots

The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots are useful when you want to create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash-consistent unless you quiesce them.

Quiesced snapshots

When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you initiate a snapshot, but are not aware of what is happening in the virtual machine and you want to have several recent backups to revert to, rather than capturing the memory, you can quiesce the files.

If the virtual machine is powered off or VMware Tools are not available, the Quiesce parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

IMPORTANT Do not use snapshots as your only backup solution or as a long-term backup solution.

Change Disk Mode to Exclude Virtual Disks from Snapshots in the vSphere Client

You can set a virtual disk to independent mode to exclude the disk from any snapshots taken of its virtual machine.

Prerequisites

Power off the virtual machine and delete any existing snapshots before you change the disk mode. Deleting a snapshot involves committing the existing data on the snapshot disk to the parent disk.

Required privileges:

- **Virtual machine.Snapshot management.Remove Snapshot**
- **Virtual machine.Configuration.Modify device settings**

Procedure

- 1 Select **Inventory > Virtual Machine > Edit Settings**.
- 2 Click the **Hardware** tab and select the hard disk to exclude.
- 3 Under **Mode**, select **Independent**.

Snapshots do not affect the state of an independent disk.

NOTE Any disk, regardless of its type, that is created after you take a snapshot does not appear if you revert to that snapshot.

- 4 Select an independent disk mode option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 5 Click **OK**.

Take a Snapshot in the vSphere Client

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. If you are suspending a virtual machine, wait until the suspend operation finishes before you take a snapshot.

When you create a memory snapshot, the snapshot captures the state of the virtual machine's memory and the virtual machine power settings. When you capture the virtual machine's memory state, the snapshot operation takes longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stored on the disk during a restore operation.

NOTE You cannot revert to a snapshot with dynamic disks, so quiesced snapshots are not used when you restore dynamic disks. Snapshot technology has no visibility into Dynamic Disks. Dynamic Disks are commonly known as Microsoft specific file systems.

Prerequisites

- If you are taking a memory snapshot of a virtual machine that has multiple disks in different disk modes, verify that the virtual machine is powered off. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- To capture the memory state of the virtual machine, verify that the virtual machine is powered on.
- To quiesce the virtual machine files, verify that the virtual machine is powered on and that VMware Tools is installed.
- Required privilege: **Virtual machine.Snapshot management. Create snapshot** on the virtual machine.

Procedure

- 1 Select **Inventory > Virtual Machine > Snapshot > Take Snapshot**.
- 2 Type a name for the snapshot.
- 3 Type a description for the snapshot.
Adding a date and time or a description, for example, "Snapshot before applying XYZ patch," can help you determine which snapshot to restore or delete.
- 4 (Optional) Select the **Snapshot the virtual machine's memory** check box to capture the memory of the virtual machine.
- 5 (Optional) Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to pause running processes on the guest operating system so that file system contents are in a known consistent state when you take the snapshot.
- 6 Click **OK**.

After you take the snapshot, you can view its status in the **Recent Tasks** field at the bottom of the vSphere Client.

Restoring Snapshots

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can restore a snapshot.

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot. If you want the virtual machine to be suspended, powered on, or powered off when you start it, make sure that it is in the correct state when you take the snapshot.

You can restore snapshots in the following ways:

Revert to Current Snapshot	Restores the parent snapshot, one level up in the hierarchy from the You are Here position. Revert to Current Snapshot activates the parent snapshot of the current state of the virtual machine.
Go To	Lets you restore any snapshot in the snapshot tree and makes that snapshot the parent snapshot of the current state of the virtual machine. Subsequent snapshots from this point create a new branch of the snapshot tree.

Restoring snapshots has the following effects:

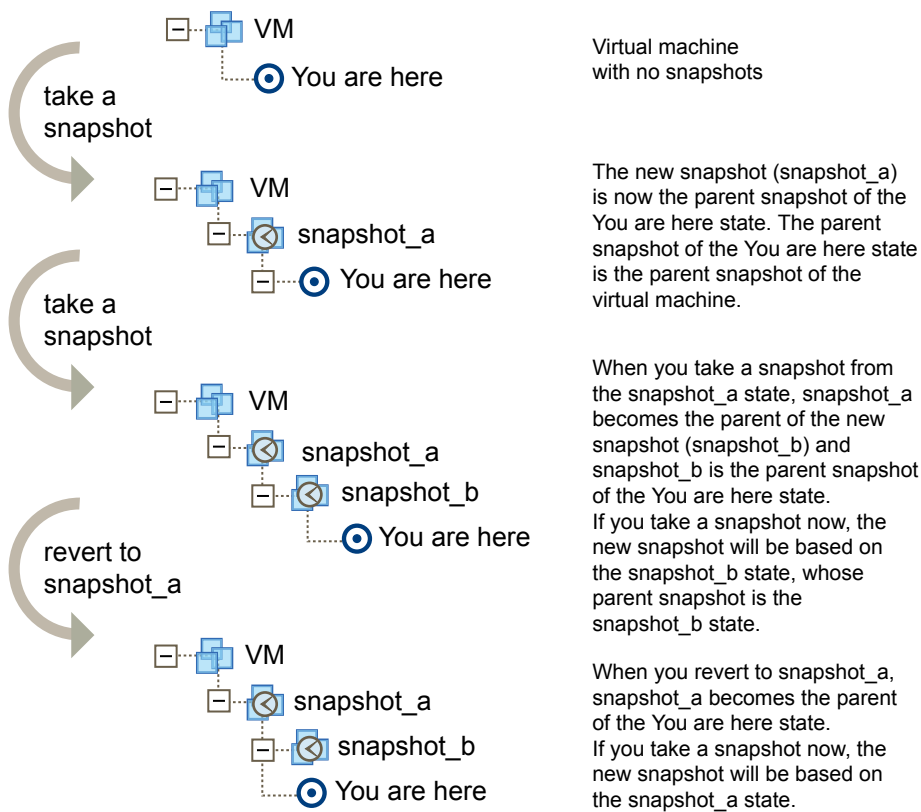
- The current disk and memory states are discarded, and the virtual machine reverts to the disk and memory states of the parent snapshot.
- Existing snapshots are not removed. You can restore those snapshots at any time.

- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.

Table 11-1. Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Figure 11-1. Revert to Snapshot

When you revert a virtual machine, the virtual machine returns to the parent snapshot of the virtual machine (that is, the parent of the current You are here state).

NOTE vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

Revert to a Snapshot in the vSphere Client

You can restore the parent snapshot of the current state of the virtual machine.

When you revert to a snapshot, disks that you added or changed after the snapshot was taken are reverted to the snapshot point. For example, when you take a snapshot of a virtual machine, add a disk, and revert the snapshot, the added disk is removed.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Revert to snapshot** on the virtual machine.

Procedure

- ◆ Right-click a virtual machine in the vSphere Client inventory and select **Revert to Current Snapshot**.

The virtual machine power and data states are returned to the states they were in at the time you took the parent snapshot. If the parent snapshot is a memory snapshot, the virtual machine is restored to an on power state.

Go To a Snapshot in the vSphere Client

You can go to any snapshot in the snapshot tree to restore the virtual machine to the state of that snapshot.

NOTE Virtual machines running certain kinds of workloads might take several minutes to resume responsiveness after reverting from a snapshot.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Revert to snapshot** on the virtual machine

Procedure

- 1 Right-click a virtual machine in the vSphere Client inventory and select **Snapshot Manager**.
- 2 In the Snapshot Manager, click a snapshot to select it.
- 3 Click **Go to** to restore the virtual machine to the snapshot.
- 4 Click **Yes** in the confirmation dialog box.

Subsequent child snapshots from this point create a new branch of the snapshot tree. The delta disks for snapshots that you took after you restored the current snapshot are not removed and you can restore those snapshots at any time.

Deleting Snapshots

Deleting a snapshot removes the snapshot from the Snapshot Manager. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk.

Deleting a snapshot leaves the current state of the virtual machine or any other snapshot untouched. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes to the parent disk all data from the delta disk that contains the information about the deleted snapshot. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

Deleting snapshots involves large amounts of disk reads and writes, which can reduce virtual machine performance until consolidation is complete. Consolidating snapshots removes redundant disks, which improves virtual machine performance and saves storage space. The time it takes to delete snapshots and consolidate the snapshot files depends on the volume of data that the guest operating system wrote to the virtual disks after you took the last snapshot. The required time is proportional to the amount of data the virtual machine is writing during consolidation if the virtual machine is powered on.

If disk consolidation fails when you delete a snapshot or delete all snapshots and you notice a degradation in virtual machine performance, you can view a list of virtual machines to determine if any files require consolidation, and if so, run a separate consolidation operation. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see [“Consolidate Snapshots in the vSphere Client,”](#) on page 121

Delete

Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes between the snapshot and the previous delta disk state to the parent snapshot.

You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.

Delete All

Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes changes between snapshots and previous delta disk states to the base parent disk and merges them with the base virtual machine disk.

To prevent snapshot files from merging with the parent snapshot, for example in cases of failed updates or installations, first use the **Go to** command to restore to a previous snapshot. This action invalidates the snapshot delta disks and deletes the memory file. You can then use the **Delete** option to remove the snapshot and any associated files.

Delete a Snapshot in the vSphere Client

You can use the Snapshot Manager to delete a single snapshot or all snapshots in a snapshot tree.

Use care when you delete snapshots. You cannot restore a deleted snapshot. For example, you might want to install several browsers, a, b, and c, and capture the virtual machine state after you install each browser. The first, or base snapshot, captures the virtual machine with browser a and the second snapshot captures browser b. If you restore the base snapshot that includes browser a and take a third snapshot to capture browser c and delete the snapshot that contains browser b, you cannot return to the virtual machine state that includes browser b.

Prerequisites

- Ensure that you are familiar with the Delete and Delete all actions and how they might affect virtual machine performance. See [“Deleting Snapshots,”](#) on page 119.
- Required Privilege: **Virtual machine.Snapshot management.Remove Snapshot** on the virtual machine.

Procedure

- 1 Select **Inventory > Virtual Machine > Snapshot > Snapshot Manager**.
- 2 In the Snapshot Manager, click a snapshot to select it.
- 3 Select a delete option.

Option	Description
Delete	Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine.
Delete All	Consolidates all of the immediate snapshots before the You are here current state to the base parent disk and removes all existing snapshots from the Snapshot Manager and virtual machine.

- 4 Click **Yes**.

Consolidate Snapshots in the vSphere Client

The snapshot Consolidation command searches for hierarchies or delta disks to combine without violating data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compact after a **Delete** or **Delete all** operation or if the disk did not consolidate. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

The Needs Consolidation column in the vSphere Client shows the virtual machines that need to be consolidated and the virtual machine's **Summary** tab shows a Configuration Issues consolidation message if the virtual machine needs to be consolidated. If you see errors for failed conditions, such as running out of disk space, correct them and run the consolidation task.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Remove Snapshot**

Procedure

- 1 Display the Need Consolidation column in the vSphere Client.
 - a Select a vCenter Server, host, or cluster and click the **Virtual Machines** tab.
 - b Right-click the menu bar for any virtual machine column and select **Needs Consolidation** from the menu.

The Needs Consolidation column appears. A Yes status indicates that the snapshot files for the virtual machine should be consolidated and that the virtual machine's **Tasks and Events** tab shows a configuration problem. A No status indicates that the files are OK.

- 2 To consolidate the files, right-click the virtual machine and select **Snapshot > Consolidate**.
- 3 Check the Need Consolidation column to verify that the task succeeded.

If the task succeeded, the Configuration Issues message should be cleared and the Needs Consolidation value should be No.

Networking in the vSphere Client

When you connect directly to a host with the vSphere Client, you view and configure vSphere Standard switches on that host.

This chapter includes the following topics:

- [“View Networking Information in the vSphere Client,”](#) on page 123
- [“View Network Adapter Information in the vSphere Client,”](#) on page 123
- [“Setting Up Networking with vSphere Standard Switches,”](#) on page 124

View Networking Information in the vSphere Client

The vSphere Client shows general networking information and information specific to network adapters.

Procedure

- 1 Log in to the vSphere Client and select the host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 (Optional) Choose the type of networking to view.

Option	Description
vSphere Standard Switch	Displays vSphere standard switch networking on the host.
vSphere Distributed Switch	Displays vSphere distributed switch networking on the host.

The **vSphere Distributed Switch** option appears only on hosts that are connected to one or more vSphere distributed switches.

Networking information is displayed for each virtual switch on the host.

View Network Adapter Information in the vSphere Client

For each physical network adapter on the host, you can view information such as the speed, duplex, and observed IP ranges.

Procedure

- 1 Log in to the vSphere Client and select the **Hosts and Clusters** inventory view.
- 2 Select the host in the inventory pane.
- 3 Click the **Configuration** tab, and click **Network Adapters**.

The network adapters panel shows the following information.

Table 12-1. Network Adapter Parameters

Option	Description
Device	Name of the network adapter.
Speed	Actual speed and duplex of the network adapter.
Configured	Configured speed and duplex of the network adapter.
Switch	vSphere standard switch or vSphere distributed switch that the network adapter is associated with.
Observed IP ranges	IP addresses that the network adapter is likely to have access to.
Wake on LAN supported	Network adapter ability to support Wake on the LAN.

Setting Up Networking with vSphere Standard Switches

vSphere standard switches handle network traffic at the host level in a vSphere environment.

Use the vSphere Client to add networking based on the categories that reflect the types of network services.

- Virtual machines
- VMkernel

Add a Virtual Machine Port Group

Virtual machine port groups provide networking for virtual machines.

Procedure

- 1 Select the host in the inventory pane.
- 2 On the host **Configuration** tab, click **Networking**.
- 3 Select the vSphere Standard Switch view.
Standard switches appear in an overview that includes a detailed layout.
- 4 On the right side of the page, click **Add Networking**.
- 5 Accept the default connection type, **Virtual Machines**, and click **Next**.
- 6 Select **Create a vSphere standard switch** or one of the listed existing standard switches and the associated physical adapters to use for this port group.

You can create a standard switch with or without Ethernet adapters.

If you create a standard switch without physical network adapters, all traffic on that switch is confined to that switch. No other hosts on the physical network or virtual machines on other standard switches can send or receive traffic over this standard switch. You might create a standard switch without physical network adapters if you want a group of virtual machines to be able to communicate with each other, but not with other hosts or with virtual machines outside the group.

- 7 Click **Next**.
- 8 In the Port Group Properties group, enter a network label that identifies the port group that you are creating.

Use network labels to identify migration-compatible connections common to two or more hosts.

- 9 (Optional) If you are using a VLAN, for **VLAN ID**, enter a number between 1 and 4094.

If you enter 0 or leave the option blank, the port group detects only untagged (non-VLAN) traffic. If you enter 4095, the port group can detect traffic on any VLAN while leaving the VLAN tags intact.

- 10 Click **Next**.
- 11 After you determine that the switch is configured correctly, click **Finish**.

Set Up VMkernel Networking on a vSphere Standard Switch

Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.

Procedure

- 1 Select the host in the inventory pane.
- 2 On the host **Configuration** tab, click **Networking**.
- 3 In the vSphere Standard Switch view, click **Add Networking**.
- 4 Select **VMkernel** and click **Next**.
- 5 Select the vSphere standard switch to use, or select **Create a vSphere standard switch** to create a new vSphere standard switch.
- 6 Select the check boxes for the network adapters for your vSphere standard switch to use.

Select adapters for each vSphere standard switch so that virtual machines or other services that connect through the adapter can reach the correct Ethernet segment. If no adapters appear under Create a new vSphere standard switch, all the network adapters in the system are being used by existing vSphere standard switches or vSphere distributed switches. You can either create a vSphere standard switch without a network adapter, or select a network adapter that an existing vSphere standard switch uses.

- 7 Click **Next**.
- 8 Select or enter a network label and a VLAN ID.

Option	Description
Network Label	A name that identifies the port group that you are creating. This is the label that you specify when you configure VMkernel services such as vMotion and IP storage and you configure a virtual adapter to be attached to this port group.
VLAN ID	Identifies the VLAN that the port group's network traffic will use.

- 9 (Optional) Select **Use this port group for vMotion** to enable this port group to advertise itself to another host as the network connection through which vMotion traffic should be sent.
- 10 (Optional) Select **Use this port group for fault tolerance logging**.
- 11 (Optional) Select **Use this port group for management traffic**.
- 12 If IPv6 is enabled on the host, select **IP (Default)**, **IPv6**, or **IP and IPv6 networking**.

This option does not appear on hosts that do not have IPv6 enabled. IPv6 configuration cannot be used with dependent hardware iSCSI adapters.

- 13 Click **Next**.

- 14 Select how to obtain IP settings.

Option	Description
Obtain IP settings automatically	Use DHCP to obtain IP settings.
Use the following IP settings	Specify IP settings manually. <ol style="list-style-type: none"> Enter the IP address and subnet mask for the VMkernel interface. Click Edit to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI. On the DNS Configuration tab, the name of the host is entered by default. The DNS server addresses that were specified during installation are also preselected, as is the domain. Click OK and click Next.

- 15 If you are using IPv6 for the VMkernel interface, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.
Obtain IPv6 addresses automatically through router advertisement	Use router advertisement to obtain IPv6 addresses.
Static IPv6 addresses	<ol style="list-style-type: none"> Click Add to add a new IPv6 address. Enter the IPv6 address and subnet prefix length, and click OK. To change the VMkernel default gateway, click Edit.

- 16 Click **Next**.
- 17 Review the information, click **Back** to change any entries, and click **Finish**.

View VMkernel Routing Information on a vSphere Standard Switch

You can view IP and IPv6 routing information, such as network, prefix, and gateway, for a VMkernel network interface on a vSphere standard switch.

Procedure

- On the host **Configuration** tab, click **Networking**.
- Click **Properties** for the standard switch associated with the VMkernel interface to view.
- On the Ports tab, select the VMkernel network adapter to view, and click **View Routing Table** under IP Settings or IPv6 Settings.

A routing table that includes network, prefix, and gateway information for the selected VMkernel network adapter appears.

Change the Number of Ports for a vSphere Standard Switch

A vSphere standard switch serves as a container for port configurations that use a common set of network adapters, including sets that contain no network adapters at all. Each virtual switch provides a finite number of ports through which virtual machines and network services can reach one or more networks.

Procedure

- Log in to the vSphere Client and select the host from the inventory panel.
- Click the **Configuration** tab and click **Networking**.
- On the right side of the page, click **Properties** for the standard switch that you want to edit.

- 4 Click the **Ports** tab.
- 5 Select the standard switch item in the Configuration list, and click **Edit**.
- 6 Click the **General** tab.
- 7 Choose the number of ports that you want to use from the drop-down menu.
- 8 Click **OK**.

What to do next

Changes will not take effect until the system is restarted.

Change the Speed of an Uplink Adapter

You can change the connection speed and duplex of an uplink adapter.

Procedure

- 1 Log in to the vSphere Client and select the host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 Select a standard switch and click **Properties**.
- 4 Click the **Network Adapters** tab.
- 5 To change the configured speed and duplex value of a network adapter, select the network adapter and click **Edit**.
- 6 To select the connection speed manually, select the speed and duplex from the drop-down menu.

Choose the connection speed manually if the NIC and a physical switch might fail to negotiate the proper connection speed. Symptoms of mismatched speed and duplex include low bandwidth or no link connectivity.

The adapter and the physical switch port it is connected to must be set to the same value, such as auto and auto or ND and ND, where ND is some speed and duplex, but not auto and ND.
- 7 Click **OK**.

Add Uplink Adapters

You can associate multiple adapters to a single vSphere standard switch to provide NIC teaming. The team can share traffic and provide failover.

Procedure

- 1 Log in to the vSphere Client and select the host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 Select a standard switch and click **Properties**.
- 4 Click the **Network Adapters** tab.
- 5 Click **Add** to launch the Add Adapter wizard.
- 6 Select one or more adapters from the list and click **Next**.

- 7 (Optional) To reorder the NICs into a different category, select a NIC and click **Move Up** and **Move Down**.

Option	Description
Active Adapters	Adapters that the standard switch uses.
Standby Adapters	Adapters that become active if one or more of the active adapters fails.

- 8 Click **Next**.
- 9 Review the information on the Adapter Summary page, click **Back** to change any entries, and click **Finish**.

The list of network adapters reappears, showing the adapters that the standard switch now claims.

- 10 Click **Close** to exit the dialog box.

The Networking section in the **Configuration** tab shows the network adapters in their designated order and categories.

Managing Storage on a Single Host

When you connect to a single host using the vSphere Client, you can perform a variety of storage management tasks, including configuring adapters, creating datastores, and viewing storage device information.

This chapter includes the following topics:

- [“Display Storage Devices for a Host in the vSphere Client,”](#) on page 130
- [“Display Storage Devices for an Adapter in the vSphere Client,”](#) on page 130
- [“View Storage Adapters Information in the vSphere Client,”](#) on page 130
- [“Review Datastore Information in the vSphere Client,”](#) on page 130
- [“Assign WWNs to Virtual Machines,”](#) on page 130
- [“Modify WWN Assignments,”](#) on page 131
- [“Set Up Networking for Software FCoE,”](#) on page 132
- [“Add Software FCoE Adapters,”](#) on page 133
- [“Disable Automatic Host Registration,”](#) on page 133
- [“Setting Up Independent Hardware iSCSI Adapters,”](#) on page 134
- [“Configuring Dependent Hardware iSCSI Adapters,”](#) on page 135
- [“Configuring Software iSCSI Adapters,”](#) on page 137
- [“Setting Up iSCSI Network,”](#) on page 138
- [“Using Jumbo Frames with iSCSI,”](#) on page 143
- [“Configuring Discovery Addresses for iSCSI Adapters,”](#) on page 144
- [“Configuring CHAP Parameters for iSCSI Adapters,”](#) on page 146
- [“Configure Advanced Parameters for iSCSI in the vSphere Client,”](#) on page 149
- [“Managing Storage Devices,”](#) on page 149
- [“Working with Datastores,”](#) on page 151

Display Storage Devices for a Host in the vSphere Client

Use the vSphere Client to display all storage devices or LUNs available to a host. If you use any third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

Procedure

- 1 Select a host and click the **Configuration** tab.
- 2 In Hardware, select **Storage**.
- 3 Click **Devices**.
- 4 To view additional details about a specific device, select the device from the list.

Display Storage Devices for an Adapter in the vSphere Client

Use the vSphere Client to display a list of storage devices accessible to a specific storage adapter on the host.

Procedure

- 1 Select a host and click the **Configuration** tab.
- 2 In Hardware, select **Storage Adapters**.
- 3 Select the adapter from the Storage Adapters list.
- 4 Click **Devices**.

View Storage Adapters Information in the vSphere Client

Use the vSphere Client to display storage adapters that your host uses and to review their information.

Procedure

- 1 Select a host and click the **Configuration** tab.
- 2 In Hardware, select **Storage Adapters**.
- 3 To view details for a specific adapter, select the adapter from the Storage Adapters list.
- 4 To list all storage devices the adapter can access, click **Devices**.
- 5 To list all paths the adapter uses, click **Paths**.

Review Datastore Information in the vSphere Client

Use the vSphere Client to display all datastores available to the hosts and analyze their properties.

Procedure

- 1 Select a host and click the **Configuration** tab.
- 2 In Hardware, select **Storage**.
- 3 Click the **Datastores** view.
- 4 To display details for a particular datastore, select the datastore from the list.

Assign WWNs to Virtual Machines

You can assign a WWN to a new virtual machine with an RDM disk when you create this virtual machine.

You can create from 1 to 16 WWN pairs, which can be mapped to the first 1 to 16 physical HBAs on the host.

Procedure

- 1 Open the New Virtual Machine wizard.
- 2 Select **Custom**, and click **Next**.
- 3 Follow all steps required to create a custom virtual machine.
- 4 On the Select a Disk page, select **Raw Device Mapping**, and click **Next**.
- 5 From a list of SAN disks or LUNs, select a raw LUN you want your virtual machine to access directly.
- 6 Select a datastore for the RDM mapping file.

You can place the RDM file on the same datastore where your virtual machine files reside, or select a different datastore.

NOTE If you want to use vMotion for a virtual machine with enabled NPIV, make sure that the RDM file is located on the same datastore where the virtual machine configuration file resides.

- 7 Follow the steps required to create a virtual machine with the RDM.
- 8 On the Ready to Complete page, select the **Edit the virtual machine settings before completion** check box and click **Continue**.

The Virtual Machine Properties dialog box opens.

- 9 Assign WWNs to the virtual machine.
 - a Click the **Options** tab, and select **Fibre Channel NPIV**.
 - b Select **Generate new WWNs**.
 - c Specify the number of WWNNs and WWPNS.

A minimum of 2 WWPNS are needed to support failover with NPIV. Typically only 1 WWNN is created for each virtual machine.

- 10 Click **Finish**.

The host creates WWN assignments for the virtual machine.

What to do next

Register newly created WWNs in the fabric so that the virtual machine is able to log in to the switch, and assign storage LUNs to the WWNs.

Modify WWN Assignments

You can modify WWN assignments for a virtual machine with an RDM.

Typically, you do not need to change existing WWN assignments on your virtual machine. In certain circumstances, for example, when manually assigned WWNs are causing conflicts on the SAN, you might need to change or remove WWNs.

Prerequisites

Make sure to power off the virtual machine if you want to edit the existing WWNs.

Before you begin, ensure that your SAN administrator has provisioned the storage LUN ACL to allow the virtual machine's ESXi host to access it.

Procedure

- 1 Open the Virtual Machine Properties dialog box by clicking the **Edit Settings** link for the selected virtual machine.

- 2 Click the **Options** tab and select **Fibre Channel NPIV**.

The Virtual Machine Properties dialog box opens.

- 3 Edit the WWN assignments by selecting one of the following options:

Option	Description
Temporarily disable NPIV for this virtual machine	Disable the WWN assignments for the virtual machine.
Leave unchanged	The existing WWN assignments are retained. The read-only WWN Assignments section of this dialog box displays the node and port values of any existing WWN assignments.
Generate new WWNs	New WWNs are generated and assigned to the virtual machine, overwriting any existing WWNs (those of the HBA itself are unaffected).
Remove WWN assignment	The WWNs assigned to the virtual machine are removed and it uses the HBA WWNs to access the storage LUN. This option is not available if you are creating a new virtual machine.

- 4 Click **OK** to save your changes.

Set Up Networking for Software FCoE

Before you activate the software FCoE adapters, you need to connect the VMkernel to physical FCoE NICs installed on your host.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 In the vSphere standard switch view, click **Add Networking**.
- 4 Select **VMkernel** and click **Next**.
- 5 Select **Create a vSphere standard switch** to create a new vSphere standard switch.
- 6 Select the network adapter (vmnic#) that supports FCoE and click **Next**.

If your host has multiple network adapters or multiple ports on the adapter, you can add all of them to a single vSphere standard switch. An alternative is to connect each FCoE NIC to a separate standard switch.

NOTE ESXi supports the maximum of four network adapter ports used for software FCoE.

- 7 Enter a network label.

Network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, FCoE.

- 8 Specify a VLAN ID and click **Next**.

Because FCoE traffic requires an isolated network, make sure that the VLAN ID you enter is different from the one used for regular networking on your host. For more information, see the *vSphere Networking* documentation.

- 9 Specify the IP settings and click **Next**.
- 10 Review the information and click **Finish**.

You have created the virtual VMkernel adapter for the physical FCoE network adapter installed on your host.

Note To avoid FCoE traffic disruptions, do not remove the FCoE network adapter (vmnic#) from the vSphere standard switch after you set up FCoE networking.

Add Software FCoE Adapters

You must activate software FCoE adapters so that your host can use them to access Fibre Channel storage.

The number of software FCoE adapters you can activate corresponds to the number of physical FCoE NIC ports on your host. ESXi supports the maximum of four software FCoE adapters on one host.

Prerequisites

Set up networking for the software FCoE adapter.

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.
- 3 Click **Add**, select **Software FCoE Adapter**, and click **OK**.
- 4 On the Add Software FCoE Adapter dialog box, select an appropriate vmnic from the drop-down list of physical network adapters.

Only those adapters that are not yet used for FCoE traffic are listed.

- 5 Click **OK**.

The software FCoE adapter appears on the list of storage adapters.

After you activate the software FCoE adapter, you can view its properties. If you do not use the adapter, you can remove it from the list of adapters.

Disable Automatic Host Registration

When you use EMC CLARiiON or Invista arrays for storage, it is required that the hosts register with the arrays. ESXi performs automatic host registration by sending the host's name and IP address to the array. If you prefer to perform manual registration using storage management software, disable the ESXi auto-registration feature.

Procedure

- 1 In the vSphere Client, select the host in the inventory panel.
- 2 Click the **Configuration** tab and click **Advanced Settings** under Software.
- 3 Click **Disk** in the left panel and scroll down to Disk.EnableNaviReg on the right.
- 4 Change the default value to 0.

This disables the automatic host registration enabled by default.

Setting Up Independent Hardware iSCSI Adapters

An independent hardware iSCSI adapter is a specialized third-party adapter capable of accessing iSCSI storage over TCP/IP. This iSCSI adapter handles all iSCSI and network processing and management for your ESXi system.

When you connect the vSphere Client directly to a host, the setup and configuration process for the independent hardware iSCSI adapters involves these steps:

- 1 Check whether the adapter needs to be licensed.
See your vendor documentation.
- 2 Install the adapter.
For installation information and information on firmware updates, see vendor documentation.
- 3 Verify that the adapter is installed correctly.
See [“View Independent Hardware iSCSI Adapters in the vSphere Client,”](#) on page 134.
- 4 Configure discovery information.
See [“Configuring Discovery Addresses for iSCSI Adapters,”](#) on page 144.
- 5 (Optional) Configure CHAP parameters.
See [“Configuring CHAP Parameters for iSCSI Adapters,”](#) on page 146.
- 6 (Optional) Enable Jumbo Frames.
See [“Using Jumbo Frames with iSCSI,”](#) on page 143.

View Independent Hardware iSCSI Adapters in the vSphere Client

View an independent hardware iSCSI adapter to verify that it is correctly installed and ready for configuration.

After you install an independent hardware iSCSI adapter, it appears on the list of storage adapters available for configuration. You can view its properties.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.
If it is installed, the hardware iSCSI adapter appears on the list of storage adapters.
- 3 Select the adapter to view.
The default details for the adapter appear, including the model, iSCSI name, iSCSI alias, IP address, and target and paths information.
- 4 Click **Properties**.
The iSCSI Initiator Properties dialog box appears. The **General** tab displays additional characteristics of the adapter.

You can now configure your independent hardware adapter or change its default characteristics.

Change Name and IP Address for Independent Hardware iSCSI Adapters

When you configure your independent hardware iSCSI adapters, make sure that their names and IP addresses are formatted properly.

Prerequisites

Required privilege: **Host .Configuration.Storage Partition Configuration**

Procedure

- 1 Access the iSCSI Initiator Properties dialog box.
- 2 Click **Configure**.
- 3 To change the default iSCSI name for your adapter, enter the new name.

Make sure the name you enter is worldwide unique and properly formatted or some storage devices might not recognize the iSCSI adapter.
- 4 (Optional) Enter the iSCSI alias.

The alias is a name that you use to identify the independent hardware iSCSI adapter.
- 5 Change the default IP settings.

You must change the default IP settings so that they are configured properly for the IP SAN. Work with your network administrator to determine the IP setting for the HBA.
- 6 Click **OK** to save your changes.

If you change the iSCSI name, it will be used for new iSCSI sessions. For existing sessions, new settings will not be used until logout and re-login.

Configuring Dependent Hardware iSCSI Adapters

A dependent hardware iSCSI adapter is a third-party adapter that depends on VMware networking, and iSCSI configuration and management interfaces provided by VMware.

An example of a dependent iSCSI adapter is a Broadcom 5709 NIC. When installed on a host, it presents its two components, a standard network adapter and an iSCSI engine, to the same port. The iSCSI engine appears on the list of storage adapters as an iSCSI adapter (vmhba). Although the iSCSI adapter is enabled by default, to make it functional, you must first connect it, through a virtual VMkernel adapter (vmk), to a physical network adapter (vmnic) associated with it. You can then configure the iSCSI adapter.

After you configure the dependent hardware iSCSI adapter, the discovery and authentication data are passed through the network connection, while the iSCSI traffic goes through the iSCSI engine, bypassing the network.

The entire setup and configuration process for the dependent hardware iSCSI adapters involves these steps:

- 1 View the dependent hardware adapters.

See [“View Dependent Hardware iSCSI Adapters,”](#) on page 136.

If your dependent hardware adapters do not appear on the list of storage adapters, check whether they need to be licensed. See your vendor documentation.
- 2 Determine the association between the dependent hardware adapters and physical NICs.

See [“Determine Association Between iSCSI and Network Adapters,”](#) on page 136.

Make sure to note the names of the corresponding physical NICs. For example, the vmhba33 adapter corresponds to vmnic1 and vmhba34 corresponds to vmnic2.

- 3 Configure networking for iSCSI.

See [“Setting Up iSCSI Network,”](#) on page 138.

Configuring the network involves creating a VMkernel interface for each physical network adapter and associating the interface with an appropriate iSCSI adapter.

- 4 (Optional) Enable Jumbo Frames.

See [“Using Jumbo Frames with iSCSI,”](#) on page 143.

- 5 Configure discovery information.

See [“Configuring Discovery Addresses for iSCSI Adapters,”](#) on page 144.

- 6 (Optional) Configure CHAP parameters.

See [“Configuring CHAP Parameters for iSCSI Adapters,”](#) on page 146.

View Dependent Hardware iSCSI Adapters

View a dependent hardware iSCSI adapter to verify that it is correctly loaded.

If the dependent hardware adapter does not appear on the list of storage adapters, check whether it needs to be licensed. See your vendor documentation.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

If it is installed, the dependent hardware iSCSI adapter appears on the list of storage adapters under such category as, for example, Broadcom iSCSI Adapter.

- 3 Select the adapter to view and click **Properties**.

The iSCSI Initiator Properties dialog box opens. It displays the default details for the adapter, including the iSCSI name, iSCSI alias, and the status.

- 4 (Optional) To change the default iSCSI name, click **Configure**.

What to do next

Although the dependent iSCSI adapter is enabled by default, to make it functional, you must set up networking for the iSCSI traffic and bind the adapter to the appropriate VMkernel iSCSI port. You then configure discovery addresses and CHAP parameters.

Determine Association Between iSCSI and Network Adapters

You create network connections to bind dependent iSCSI and network adapters. To create the connections correctly, you must determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

- 2 Click **Add**.

The network adapter, for example vmnic2, that corresponds to the dependent iSCSI adapter is listed.

What to do next

You must bind the associated dependent hardware iSCSI and network adapters by creating the network connections.

Configuring Software iSCSI Adapters

With the software-based iSCSI implementation, you can use standard NICs to connect your host to a remote iSCSI target on the IP network. The software iSCSI adapter that is built into ESXi facilitates this connection by communicating with the physical NICs through the network stack.

Before you can use the software iSCSI adapter, you must set up networking, activate the adapter, and configure parameters such as discovery addresses and CHAP.

NOTE Designate a separate network adapter for iSCSI. Do not use iSCSI on 100Mbps or slower adapters.

The software iSCSI adapter configuration workflow includes these steps:

- 1 Activate the software iSCSI adapter.
See [“Activate the Software iSCSI Adapter in the vSphere Client,”](#) on page 137.
- 2 Configure networking for iSCSI.
See [“Setting Up iSCSI Network,”](#) on page 138.
Configuring the network involves creating a VMkernel interface for each physical network adapter that you use for iSCSI and associating all interfaces with the software iSCSI adapter.
- 3 (Optional) Enable Jumbo Frames.
See [“Using Jumbo Frames with iSCSI,”](#) on page 143.
- 4 Configure discovery information.
See [“Configuring Discovery Addresses for iSCSI Adapters,”](#) on page 144.
- 5 (Optional) Configure CHAP parameters.
See [“Configuring CHAP Parameters for iSCSI Adapters,”](#) on page 146.

Activate the Software iSCSI Adapter in the vSphere Client

You must activate your software iSCSI adapter so that your host can use it to access iSCSI storage.

You can activate only one software iSCSI adapter.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

NOTE If you boot from iSCSI using the software iSCSI adapter, the adapter is enabled and the network configuration is created at the first boot. If you disable the adapter, it is reenabled each time you boot the host.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

- 3 Click **Add** and select **Software iSCSI Adapter**.

The software iSCSI adapter appears on the list of storage adapters.

- 4 Select the iSCSI adapter from the list and click **Properties**.
- 5 Click **Configure**.
- 6 Make sure that the adapter is enabled and click **OK**.

After enabling the adapter, the host assigns the default iSCSI name to it. If you change the default name, follow iSCSI naming conventions.

Disable Software iSCSI Adapter in the vSphere Client

Use the vSphere Client to disable the software iSCSI adapter if you do not need it.

Note If you disable the adapter that is used for software iSCSI boot, the adapter is reenabled each time you boot the host.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.
- 3 Select the software iSCSI adapter from the list of storage adapters and click **Properties**.
- 4 Click **Configure**.
- 5 To disable the adapter, deselect **Enabled** and click **OK**.
- 6 Reboot the host.

After reboot, the adapter no longer appears on the list of storage adapters.

The status indicates that the adapter is disabled.

Setting Up iSCSI Network

Software and dependent hardware iSCSI adapters depend on VMkernel networking. If you use the software or dependent hardware iSCSI adapters, you must configure connections for the traffic between the iSCSI component and the physical network adapters.

Configuring the network connection involves creating a virtual VMkernel interface for each physical network adapter and associating the interface with an appropriate iSCSI adapter.

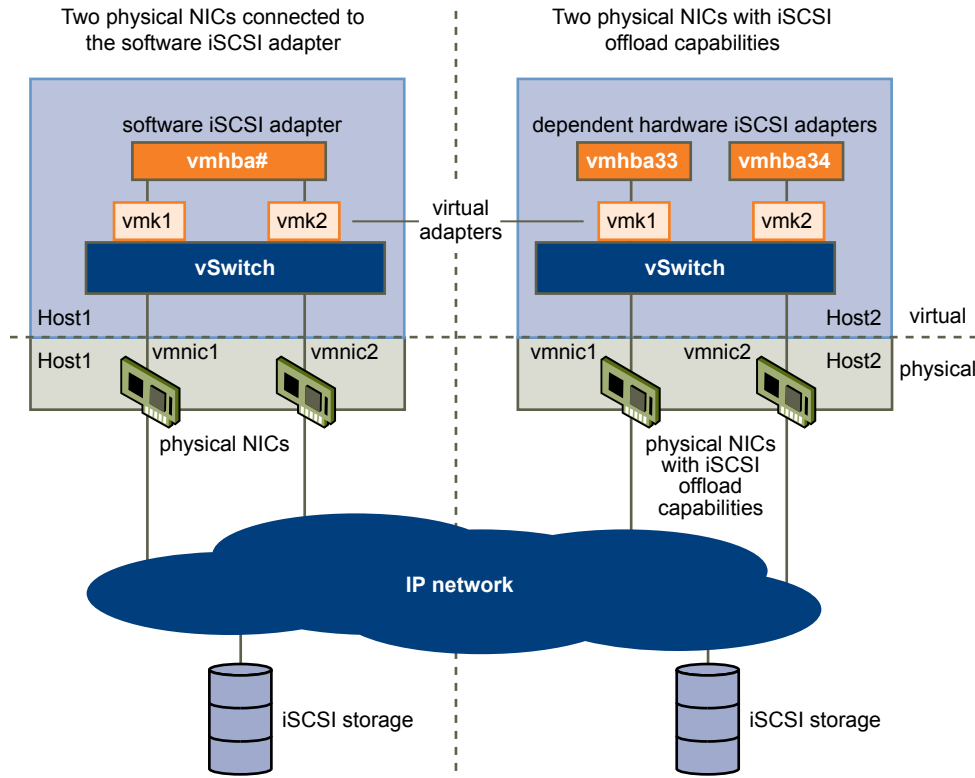
For specific considerations on when and how to use network connections with software iSCSI, see the VMware knowledge base article at <http://kb.vmware.com/kb/2038869>.

Multiple Network Adapters in iSCSI Configuration

If your host has more than one physical network adapter for software and dependent hardware iSCSI, use the adapters for multipathing.

You can connect the software iSCSI adapter with any physical NICs available on your host. The dependent iSCSI adapters must be connected only to their own physical NICs.

Note Physical NICs must be on the same subnet as the iSCSI storage system they connect to.

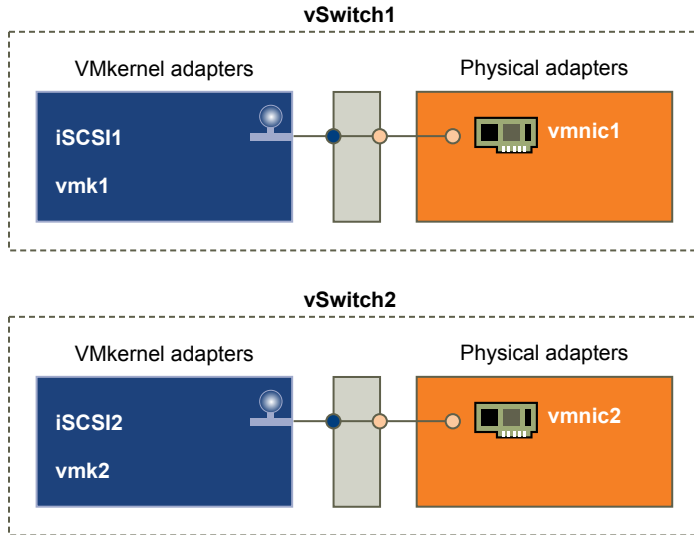
Figure 13-1. Networking with iSCSI

The iSCSI adapter and physical NIC connect through a virtual VMkernel adapter, also called virtual network adapter or VMkernel port. You create a VMkernel adapter (vmk) on a vSphere switch (vSwitch) using 1:1 mapping between each virtual and physical network adapter.

One way to achieve the 1:1 mapping when you have multiple NICs, is to designate a separate vSphere switch for each virtual-to-physical adapter pair.

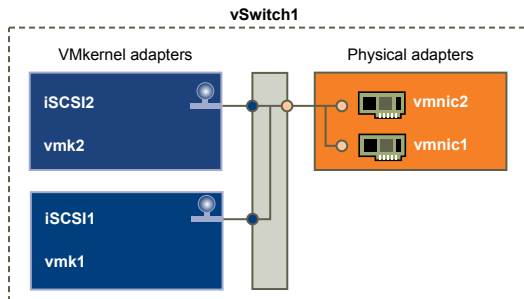
NOTE If you use separate vSphere switches, you must connect them to different IP subnets. Otherwise, VMkernel adapters might experience connectivity problems and the host will fail to discover iSCSI LUNs.

The following examples show configurations that use vSphere standard switches, but you can use distributed switches as well. For more information about vSphere distributed switches, see the *vSphere Networking* documentation.

Figure 13-2. 1:1 adapter mapping on separate vSphere standard switches

An alternative is to add all NICs and VMkernel adapters to a single vSphere standard switch. In this case, you must override the default network setup and make sure that each VMkernel adapter maps to only one corresponding active physical adapter.

NOTE You must use the single vSwitch configuration if VMkernel adapters are on the same subnet.

Figure 13-3. 1:1 adapter mapping on a single vSphere standard switch

The following table summarises the iSCSI networking configuration discussed in this topic.

Table 13-1. Networking configuration for iSCSI

iSCSI Adapters	VMkernel Adapters (Ports)	Physical Adapters (NICs)
Software iSCSI		
vmhba32	vmk1	vmnic1
	vmk2	vmnic2
Dependent Hardware iSCSI		
vmhba33	vmk1	vmnic1
vmhba34	vmk2	vmnic2

Create Network Connections for iSCSI in the vSphere Client

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

The following tasks discuss the iSCSI network configuration with a vSphere standard switch.

If you use a vSphere distributed switch with multiple uplink ports, for port binding, create a separate distributed port group per each physical NIC. Then set the team policy so that each distributed port group has only one active uplink port. For detailed information on vSphere distributed switches, see the *vSphere Networking* documentation.

Create a Single VMkernel Adapter for iSCSI

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 In the vSphere Standard Switch view, click **Add Networking**.
- 4 Select **VMkernel** and click **Next**.
- 5 Select **Create a vSphere standard switch** to create a new standard switch.
- 6 Select a NIC to use for iSCSI traffic.

IMPORTANT If you are creating a VMkernel interface for the dependent hardware iSCSI adapter, select the NIC that corresponds to the iSCSI component. See [“Determine Association Between iSCSI and Network Adapters,”](#) on page 136.

- 7 Click **Next**.
- 8 Enter a network label.

A network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, iSCSI.
- 9 Click **Next**.
- 10 Specify the IP settings and click **Next**.
- 11 Review the information and click **Finish**.

You created the virtual VMkernel adapter for a physical network adapter on your host.

What to do next

If your host has one physical network adapter for iSCSI traffic, you must bind the virtual adapter that you created to the iSCSI adapter.

If you have multiple network adapters, create additional VMkernel adapters and then perform iSCSI binding. The number of virtual adapters must correspond to the number of physical adapters on the host.

Create Additional VMkernel Adapters for iSCSI

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

Prerequisites

You must create a vSphere standard switch that maps an iSCSI VMkernel adapter to a single physical NIC designated for iSCSI traffic.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.

- 3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.
- 4 Connect additional network adapters to the standard switch.
 - a In the standard switch Properties dialog box, click the **Network Adapters** tab and click **Add**.
 - b Select one or more NICs from the list and click **Next**.
 With dependent hardware iSCSI adapters, select only those NICs that have a corresponding iSCSI component.
 - c Review the information on the Adapter Summary page and click **Finish**.
 The list of network adapters reappears, showing the network adapters that the vSphere standard switch now claims.
- 5 Create iSCSI VMkernel adapters for all NICs that you added.
 The number of VMkernel interfaces must correspond to the number of NICs on the vSphere standard switch.
 - a In the standard switch Properties dialog box, click the **Ports** tab and click **Add**.
 - b Select **VMkernel** and click **Next**.
 - c Under **Port Group Properties**, enter a network label, for example iSCSI, and click **Next**.
 - d Specify the IP settings and click **Next**.
 When you enter the subnet mask, make sure that the NIC is set to the subnet of the storage system it connects to.
 - e Review the information and click **Finish**.



CAUTION If the NIC you use with your iSCSI adapter, either software or dependent hardware, is not in the same subnet as your iSCSI target, your host cannot establish sessions from this network adapter to the target.

What to do next

Change the network policy for all VMkernel adapters, so that it is compatible with the network binding requirements. You can then bind the iSCSI VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Change Port Group Policy for iSCSI VMkernel Adapters

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

By default, for each virtual adapter on the vSphere standard switch, all network adapters appear as active. You must override this setup, so that each VMkernel interface maps to only one corresponding active NIC. For example, vmk1 maps to vmnic1, vmk2 maps to vmnic2, and so on.

Prerequisites

Create a vSphere standard switch that connects VMkernel with physical network adapters designated for iSCSI traffic. The number of VMkernel adapters must correspond to the number of physical adapters on the vSphere standard switch.

Procedure

- 1 Log in to the vSphere Client and select the host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

- 4 On the **Ports** tab, select an iSCSI VMkernel adapter and click **Edit**.
- 5 Click the **NIC Teaming** tab and select **Override switch failover order**.
- 6 Designate only one physical adapter as active and move all remaining adapters to the **Unused Adapters** category.
- 7 Repeat [Step 4](#) through [Step 6](#) for each iSCSI VMkernel interface on the vSphere standard switch.

What to do next

After you perform this task, bind the virtual VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Bind iSCSI Adapters with VMkernel Adapters in the vSphere Client

Bind an iSCSI adapter with a VMkernel adapter.

Prerequisites

Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.
The list of available storage adapters appears.
- 3 Select the software or dependent iSCSI adapter to configure and click **Properties**.
- 4 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.
- 5 Click **Add** and select a VMkernel adapter to bind with the iSCSI adapter.
You can bind the software iSCSI adapter to one or more VMkernel adapters. For a dependent hardware iSCSI adapter, only one VMkernel interface associated with the correct physical NIC is available.
- 6 Click **OK**.
The network connection appears on the list of VMkernel port bindings for the iSCSI adapter.
- 7 Verify that the network policy for the connection is compliant with the binding requirements.

Using Jumbo Frames with iSCSI

ESXi supports the use of Jumbo Frames with iSCSI.

Jumbo Frames are Ethernet frames with the size that exceeds 1500 Bytes. The maximum transmission unit (MTU) parameter is typically used to measure the size of Jumbo Frames. ESXi allows Jumbo Frames with the MTU up to 9000 Bytes.

When you use Jumbo Frames for iSCSI traffic, the following considerations apply:

- The network must support Jumbo Frames end-to-end for Jumbo Frames to be effective.
- Check with your vendors to ensure your physical NICs and iSCSI HBAs support Jumbo Frames.
- To set up and verify physical network switches for Jumbo Frames, consult your vendor documentation.

The following table explains the level of support that ESXi provides to Jumbo Frames.

Table 13-2. Support of Jumbo Frames

Type of iSCSI Adapters	Jumbo Frames Support
Software iSCSI	Supported
Dependent Hardware iSCSI	Supported. Check with vendor.
Independent Hardware iSCSI	Supported. Check with vendor.

Enable Jumbo Frames for iSCSI

Use the vSphere Client to enable Jumbo Frames for each vSphere standard switch and VMkernel adapter designated for iSCSI traffic.

Enable Jumbo Frames on the Standard switch and VMkernel adapter by changing the maximum transmission units (MTU) parameter.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Networking**.
- 3 Click **Properties** for the standard switch you use for iSCSI traffic.
- 4 On the Ports tab, select the standard switch and click **Edit**.
- 5 Set the MTU parameter for the standard switch, and click **OK**.

This step sets the MTU for all physical NICs on that standard switch. The MTU value should be set to the largest MTU size among all NICs connected to the standard switch.

- 6 On the Ports tab, select the VMkernel adapter and click **Edit**.
- 7 Set the MTU to match the value configured on the standard switch, and click **OK**.

Configuring Discovery Addresses for iSCSI Adapters

Set up target discovery addresses so that the iSCSI adapter can determine which storage resource on the network is available for access.

The ESXi system supports these discovery methods:

Dynamic Discovery

Also known as SendTargets discovery. Each time the initiator contacts a specified iSCSI server, the initiator sends the SendTargets request to the server. The server responds by supplying a list of available targets to the initiator. The names and IP addresses of these targets appear on the **Static Discovery** tab. If you remove a static target added by dynamic discovery, the target might be returned to the list the next time a rescan happens, the HBA is reset, or the host is rebooted.

Static Discovery

The initiator does not have to perform any discovery. The initiator has a list of targets it can contact and uses their IP addresses and target names to communicate with them.

Set Up Dynamic Discovery in the vSphere Client

With Dynamic Discovery, each time the initiator contacts a specified iSCSI storage system, it sends the SendTargets request to the system. The iSCSI system responds by supplying a list of available targets to the initiator.

Required privilege: **Host.Configuration.Storage Partition Configuration**

When you set up Dynamic Discovery, you can only add a new iSCSI system. You cannot change the IP address, DNS name, or port number of an existing iSCSI system. To make changes, delete the existing system and add a new one.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.
The list of available storage adapters appears.
- 3 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.
The list of available storage adapters appears.
- 4 Select the iSCSI initiator to configure, and click **Properties**.
- 5 Click the **Dynamic Discovery** tab.
- 6 To add an address for the SendTargets discovery, click **Add**.
- 7 Type the IP address or DNS name of the storage system and click **OK**.
After your host establishes the SendTargets session with this system, any newly discovered targets appear in the Static Discovery list.
- 8 To delete a specific SendTargets server, select it and click **Remove**.
After you remove a SendTargets server, it might still appear in the Inheritance field as the parent of static targets. This entry indicates where the static targets were discovered and does not affect the functionality.

What to do next

After configuring Dynamic Discovery for your iSCSI adapter, rescan the adapter.

Set Up Static Discovery in the vSphere Client

With iSCSI initiators, in addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets.

Required privilege: **Host.Configuration.Storage Partition Configuration**

When you set up Static Discovery, you can only add new iSCSI targets. You cannot change the IP address, DNS name, iSCSI target name, or port number of an existing target. To make changes, remove the existing target and add a new one.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.
The list of available storage adapters appears.
- 3 Select the iSCSI initiator to configure and click **Properties**.
- 4 Click the **Static Discovery** tab.
The tab displays all dynamically discovered targets and any static targets already entered.
- 5 To add a target, click **Add** and enter the target's information.
- 6 To delete a specific target, select the target and click **Remove**.

What to do next

After configuring Static Discovery for your iSCSI adapter, rescan the adapter.

Configuring CHAP Parameters for iSCSI Adapters

Because the IP networks that the iSCSI technology uses to connect to remote targets do not protect the data they transport, you must ensure security of the connection. One of the protocols that iSCSI implements is the Challenge Handshake Authentication Protocol (CHAP), which verifies the legitimacy of initiators that access targets on the network.

CHAP uses a three-way handshake algorithm to verify the identity of your host and, if applicable, of the iSCSI target when the host and target establish a connection. The verification is based on a predefined private value, or CHAP secret, that the initiator and target share.

ESXi supports CHAP authentication at the adapter level. In this case, all targets receive the same CHAP name and secret from the iSCSI initiator. For software and dependent hardware iSCSI adapters, ESXi also supports per-target CHAP authentication, which allows you to configure different credentials for each target to achieve greater level of security.

Set Up CHAP for iSCSI Adapter in the vSphere Client

You can set up all targets to receive the same CHAP name and secret from the iSCSI initiator at the initiator level. By default, all discovery addresses or static targets inherit CHAP parameters that you set up at the initiator level.

The CHAP name should not exceed 511 alphanumeric characters and the CHAP secret should not exceed 255 alphanumeric characters. Some adapters, for example the QLogic adapter, might have lower limits, 255 for the CHAP name and 100 for the CHAP secret.

Prerequisites

- Before setting up CHAP parameters for software or dependent hardware iSCSI, determine whether to configure one-way or mutual CHAP. Independent hardware iSCSI adapters do not support mutual CHAP.
 - In one-way CHAP, the target authenticates the initiator.
 - In mutual CHAP, both the target and the initiator authenticate each other. Use different secrets for CHAP and mutual CHAP.

When you configure CHAP parameters, verify that they match the parameters on the storage side.

- Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Access the iSCSI Initiator Properties dialog box.
- 2 On the **General** tab, click **CHAP**.

- 3 To configure one-way CHAP, under CHAP specify the following:
 - a Select the CHAP security level.
 - Do not use CHAP unless required by target (software and dependent hardware iSCSI only)
 - Use CHAP unless prohibited by target
 - Use CHAP (software and dependent hardware iSCSI only). To configure mutual CHAP, you must select this option.
 - b Specify the CHAP name.

Make sure that the name you specify matches the name configured on the storage side.

 - To set the CHAP name to the iSCSI initiator name, select **Use initiator name**.
 - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and type a name in the **Name** text box.
 - c Enter a one-way CHAP secret to be used as part of authentication. Use the same secret that you enter on the storage side.
- 4 To configure mutual CHAP, first configure one-way CHAP by following the directions in [Step 3](#).

Make sure to select **Use CHAP** as an option for one-way CHAP. Then, specify the following under **Mutual CHAP**:

 - a Select **Use CHAP**.
 - b Specify the mutual CHAP name.
 - c Enter the mutual CHAP secret. Make sure to use different secrets for the one-way CHAP and mutual CHAP.
- 5 Click **OK**.
- 6 Rescan the initiator.

If you change the CHAP or mutual CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and log in again.

Set Up CHAP for Target in the vSphere Client

For software and dependent hardware iSCSI adapters, you can configure different CHAP credentials for each discovery address or static target.

When configuring CHAP parameters, make sure that they match the parameters on the storage side. The CHAP name should not exceed 511 and the CHAP secret 255 alphanumeric characters.

Required privilege: **Host.Configuration.Storage Partition Configuration**

Prerequisites

Before setting up CHAP parameters for software and dependent hardware iSCSI, determine whether to configure one-way or mutual CHAP.

- In one-way CHAP, the target authenticates the initiator.
- In mutual CHAP, both the target and initiator authenticate each other. Make sure to use different secrets for CHAP and mutual CHAP.

Procedure

- 1 Access the iSCSI Initiator Properties dialog box.
- 2 Select either **Dynamic Discovery** tab or **Static Discovery** tab.

- 3 From the list of available targets, select a target you want to configure and click **Settings > CHAP**.
- 4 Configure one-way CHAP in the CHAP area.
 - a Deselect **Inherit from parent**.
 - b Select one of the following options:
 - Do not use CHAP unless required by target
 - Use CHAP unless prohibited by target
 - Use CHAP. To be able to configure mutual CHAP, you must select this option.
 - c Specify the CHAP name.
Make sure that the name you specify matches the name configured on the storage side.
 - To set the CHAP name to the iSCSI initiator name, select **Use initiator name**.
 - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and enter a name in the **Name** field.
 - d Enter a one-way CHAP secret to be used as part of authentication. Make sure to use the same secret that you enter on the storage side.
- 5 To configure mutual CHAP, first configure one-way CHAP by following directions in [Step 4](#).
Make sure to select **Use CHAP** as an option for one-way CHAP. Then, specify the following in the Mutual CHAP area:
 - a Deselect **Inherit from parent**.
 - b Select **Use CHAP**.
 - c Specify the mutual CHAP name.
 - d Enter the mutual CHAP secret. Make sure to use different secrets for the one-way CHAP and mutual CHAP.
- 6 Click **OK**.
- 7 Rescan the initiator.

If you change the CHAP or mutual CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and login again.

Disable CHAP

You can disable CHAP if your storage system does not require it.

If you disable CHAP on a system that requires CHAP authentication, existing iSCSI sessions remain active until you reboot your host, end the session through the command line, or the storage system forces a logout. After the session ends, you can no longer connect to targets that require CHAP.

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Open the CHAP Credentials dialog box.
- 2 For software and dependent hardware iSCSI adapters, to disable just the mutual CHAP and leave the one-way CHAP, select **Do not use CHAP** in the Mutual CHAP area.
- 3 To disable one-way CHAP, select **Do not use CHAP** in the CHAP area.

The mutual CHAP, if set up, automatically turns to **Do not use CHAP** when you disable the one-way CHAP.

- 4 Click **OK**.

Configure Advanced Parameters for iSCSI in the vSphere Client

The advanced iSCSI settings control such parameters as header and data digest, ARP redirection, delayed ACK, and so on. Generally, you do not need to change these settings because your host works with the assigned predefined values.



CAUTION Do not make any changes to the advanced iSCSI settings unless you are working with the VMware support team or otherwise have thorough information about the values to provide for the settings.

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Access the iSCSI Initiator Properties dialog box.
- 2 To configure advanced parameters at the initiator level, on the General tab, click **Advanced**. Proceed to [Step 4](#).
- 3 Configure advanced parameters at the target level.
At the target level, advanced parameters can be configured only for software and dependent hardware iSCSI adapters.
 - a Select either the **Dynamic Discovery** tab or **Static Discovery** tab.
 - b From the list of available targets, select a target to configure and click **Settings > Advanced**.
- 4 Enter any required values for the advanced parameters you want to modify and click **OK** to save your changes.

Managing Storage Devices

Manage local and networked storage device that your ESXi host has access to.

Rename Storage Devices in the vSphere Client

You can change the display name of a storage device. The display name is assigned by the ESXi host based on the storage type and manufacturer.

Procedure

- 1 Select the host in the vSphere Client inventory.
- 2 Click the **Configuration** tab.
- 3 Click **Storage** and then click **Devices**.
- 4 Right-click the device to rename and select **Rename**.
- 5 Change the device name to a friendly name.

Perform Storage Rescan in the vSphere Client

When you make changes in your SAN configuration, you might need to rescan your storage. You can rescan all storage available to your host. If the changes you make are isolated to storage accessed through a specific adapter, perform rescan for only this adapter.

Use this procedure if you want to limit the rescan to storage available to a particular host or accessed through a particular adapter on the host. If you want to rescan storage available to all hosts managed by your vCenter Server system, you can do so by right-clicking a datacenter, cluster, or folder that contains the hosts and selecting **Rescan for Datastores**.

Procedure

- 1 In the vSphere Client, select a host and click the **Configuration** tab.
- 2 Select a rescan option.

Option	Description
Storage	In the Hardware panel, click Storage , and click Rescan All above the Datastores or Devices panel.
Storage Adapters	In the Hardware panel, click Storage Adapters , and click Rescan All above the Storage Adapters panel. NOTE You can also right-click an individual adapter and select Rescan to rescan just that adapter.

- 3 Specify extent of rescan.

Option	Description
Scan for New Storage Devices	Rescan all adapters to discover new storage devices. If new devices are discovered, they appear in the device list.
Scan for New VMFS Volumes	Rescan all storage devices to discover new datastores that have been added since the last scan. Any new datastores appear in the datastore list.

Change the Number of Scanned LUNs

By default, the VMkernel scans for LUN 0 to LUN 255 for every target (a total of 256 LUNs). You can modify the **Disk.MaxLUN** parameter to improve LUN discovery speed.

IMPORTANT You cannot discover LUNs with a LUN ID number that is greater than 255.

Reducing the value can shorten rescan time and boot time. However, the time to rescan LUNs might depend on other factors, including the type of storage system and whether sparse LUN support is enabled.

Procedure

- 1 In the vSphere Client inventory panel, select the host, click the **Configuration** tab, and click **Advanced Settings** under Software.
- 2 Select **Disk**.
- 3 Scroll down to **Disk.MaxLUN**.
- 4 Change the existing value to the value of your choice, and click **OK**.

The value you enter specifies the LUN after the last one you want to discover.

For example, to discover LUNs from 0 through 31, set **Disk.MaxLUN** to 32.

Working with Datastores

Datastores are logical containers, analogous to file systems, that hide specifics of each storage device and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

You use the vSphere Client to access different types of storage devices that your ESXi host discovers and to deploy datastores on them.

Depending on the type of storage you use, datastores can be backed by the following file system formats:

- Virtual Machine File System (VMFS)
- Network File System (NFS)

After creating datastores, you can organize them in different ways. For example, you can group them into folders according to business practices. This allows you to assign the same permissions and alarms on the datastores in the group at one time.

You can also add datastores to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create a datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the *vSphere Resource Management* documentation.

Create a VMFS Datastore in the vSphere Client

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

Prerequisites

Before creating datastores, you must install and configure any adapters that your storage requires. Rescan the adapters to discover newly added storage devices.

Procedure

- 1 Log in to the vSphere Client and select the host from the Inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Datastores** and click **Add Storage**.
- 4 Select the **Disk/LUN** storage type and click **Next**.
- 5 Select a device to use for your datastore and click **Next**.

IMPORTANT Select the device that does not have a datastore name displayed in the VMFS Label column. If a name is present, the device contains a copy of an existing VMFS datastore.

- 6 Select the **File System Version** and click **Next**.

IMPORTANT If you select VMFS3 you must select the maximum file size under **Formatting**.

- 7 If the disk is not blank, review the current disk layout in the top panel of the Current Disk Layout page and select a configuration option from the bottom panel.

Option	Description
Use all available partitions	Dedicates the entire disk to a single VMFS datastore. If you select this option, all file systems and data currently stored on this device are destroyed.
Use free space	Deploys a VMFS datastore in the remaining free space of the disk.

If the disk you are formatting is blank, the **Current Disk Layout** page presents the entire disk space for storage configuration.

- 8 Click **Next**.
- 9 On the **Properties** page, type a datastore name and click **Next**.
- 10 If the space specified for storage is excessive for your purposes, you can adjust the capacity values.
By default, the entire free space on the storage device is available.
- 11 Click **Next**.
- 12 In the Ready to Complete page, review the datastore configuration information and click **Finish**.

A datastore on the SCSI-based storage device is created. If you use the vCenter Server system to manage your hosts, the newly created datastore is added to all hosts.

Create NFS Datastores

You can use the Add Storage wizard to mount an NFS volume and use it as if it were a VMFS datastore.

Prerequisites

Because NFS requires network connectivity to access data stored on remote servers, before configuring NFS, you must first configure VMkernel networking.

Procedure

- 1 Log in to the vSphere Client and select the host from the Inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Datastores** and click **Add Storage**.
- 4 Select **Network File System** as the storage type and click **Next**.
- 5 Enter the server name, the mount point folder name, and the datastore name.

For the server name, you can enter an IP address, a DNS name, or an NFS UUID.

NOTE When you mount the same NFS volume on different hosts, make sure that the server and folder names are identical across the hosts. If the names do not match exactly, the hosts see the same NFS volume as two different datastores. This might result in a failure of such features as vMotion. An example of such discrepancy could be if you enter **filer** as the server name on one host and **filer.domain.com** on the other.

- 6 (Optional) Select **Mount NFS read only** if the volume is exported as read only by the NFS server.
- 7 Click **Next**.
- 8 In the Network File System Summary page, review the configuration options and click **Finish**.

Managing Duplicate VMFS Datastores

When a storage device contains a VMFS datastore copy, you can mount the datastore with the existing signature or assign a new signature.

Each VMFS datastore created in a storage disk has a unique signature, also called UUID, that is stored in the file system superblock. When the storage disk is replicated or its snapshot is taken on the storage side, the resulting disk copy is identical, byte-for-byte, with the original disk. As a result, if the original storage disk contains a VMFS datastore with UUID X, the disk copy appears to contain an identical VMFS datastore, or a VMFS datastore copy, with exactly the same UUID X.

In addition to LUN snapshotting and replication, the following storage device operations might cause ESXi to mark the existing datastore on the device as a copy of the original datastore:

- LUN ID changes
- SCSI device type changes, for example, from SCSI-2 to SCSI-3
- SPC-2 compliancy enablement

ESXi can detect the VMFS datastore copy and display it in the vSphere Web Client. You have an option of mounting the datastore copy with its original UUID or changing the UUID to resignature the datastore.

Whether you chose resignaturing or mounting without resignaturing depends on how the LUNs are masked in the storage environment. If your hosts are able to see both copies of the LUN, then resignaturing is the recommended method. Otherwise, mounting is an option.

Mount a VMFS Datastore with an Existing Signature

If you do not need to resignature a VMFS datastore copy, you can mount it without changing its signature.

You can keep the signature if, for example, you maintain synchronized copies of virtual machines at a secondary site as part of a disaster recovery plan. In the event of a disaster at the primary site, you mount the datastore copy and power on the virtual machines at the secondary site.

IMPORTANT You can mount a VMFS datastore copy only if it does not collide with the original VMFS datastore that has the same UUID. To mount the copy, the original VMFS datastore has to be offline.

When you mount the VMFS datastore, ESXi allows both reads and writes to the datastore residing on the LUN copy. The LUN copy must be writable. The datastore mounts are persistent and valid across system reboots.

Prerequisites

Before you mount a VMFS datastore, perform a storage rescan on your host so that it updates its view of LUNs presented to it.

Procedure

- 1 Log in to the vSphere Client and select the server from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Add Storage**.
- 4 Select the **Disk/LUN** storage type and click **Next**.
- 5 From the list of LUNs, select the LUN that has a datastore name displayed in the VMFS Label column and click **Next**.

The name present in the VMFS Label column indicates that the LUN is a copy that contains a copy of an existing VMFS datastore.

- 6 Under Mount Options, select **Keep Existing Signature**.
- 7 In the Ready to Complete page, review the datastore configuration information and click **Finish**.

What to do next

If you later want to resignature the mounted datastore, you must unmount it first.

Resignature a VMFS Datastore Copy

Use datastore resignaturing if you want to retain the data stored on the VMFS datastore copy.

When resignaturing a VMFS copy, ESXi assigns a new UUID and a new label to the copy, and mounts the copy as a datastore distinct from the original.

The default format of the new label assigned to the datastore is *snap-snapID-oldLabel*, where *snapID* is an integer and *oldLabel* is the label of the original datastore.

When you perform datastore resignaturing, consider the following points:

- Datastore resignaturing is irreversible.
- The LUN copy that contains the VMFS datastore that you resignature is no longer treated as a LUN copy.
- A spanned datastore can be resignatured only if all its extents are online.
- The resignaturing process is crash and fault tolerant. If the process is interrupted, you can resume it later.
- You can mount the new VMFS datastore without a risk of its UUID colliding with UUIDs of any other datastore, such as an ancestor or child in a hierarchy of LUN snapshots.

Prerequisites

To resignature a mounted datastore copy, first unmount it.

Before you resignature a VMFS datastore, perform a storage rescan on your host so that the host updates its view of LUNs presented to it and discovers any LUN copies.

Procedure

- 1 Log in to the vSphere Client and select the server from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Add Storage**.
- 4 Select the **Disk/LUN** storage type and click **Next**.
- 5 From the list of LUNs, select the LUN that has a datastore name displayed in the VMFS Label column and click **Next**.

The name present in the VMFS Label column indicates that the LUN is a copy that contains a copy of an existing VMFS datastore.

- 6 Under Mount Options, select **Assign a New Signature** and click **Next**.
- 7 In the Ready to Complete page, review the datastore configuration information and click **Finish**.

What to do next

After resignaturing, you might have to do the following:

- If the resignatured datastore contains virtual machines, update references to the original VMFS datastore in the virtual machine files, including *.vmx*, *.vmdk*, *.vmsd*, and *.vmsn*.
- To power on virtual machines, register them with vCenter Server.

Upgrading VMFS Datastores

If your datastores were formatted with VMFS2 or VMFS3, you can upgrade the datastores to VMFS5.

When you perform datastore upgrades, consider the following items:

- To upgrade a VMFS2 datastore, you use a two-step process that involves upgrading VMFS2 to VMFS3 first. Because ESXi 5.0 and later hosts cannot access VMFS2 datastores, use a legacy host, ESX/ESXi 4.x or earlier, to access the VMFS2 datastore and perform the VMFS2 to VMFS3 upgrade.

After you upgrade your VMFS2 datastore to VMFS3, the datastore becomes available on the ESXi 5.x host, where you complete the process of upgrading to VMFS5.

- You can perform a VMFS3 to VMFS5 upgrade while the datastore is in use with virtual machines powered on.
- While performing an upgrade, your host preserves all files on the datastore.
- The datastore upgrade is a one-way process. After upgrading your datastore, you cannot revert it back to its previous VMFS format.

An upgraded VMFS5 datastore differs from a newly formatted VMFS5.

Table 13-3. Comparing Upgraded and Newly Formatted VMFS5 Datastores

Characteristics	Upgraded VMFS5	Formatted VMFS5
File block size	1, 2, 4, and 8MB	1MB
Subblock size	64KB	8KB
Partition format	MBR. Conversion to GPT happens only after you expand the datastore to a size larger than 2TB.	GPT
Datastore limits	Retains limits of VMFS3 datastore.	

Upgrade VMFS2 Datastores to VMFS3

If your datastore was formatted with VMFS2, you must first upgrade it to VMFS3. Because ESXi 5.x hosts cannot access VMFS2 datastores, use a legacy host, ESX/ESXi 4.x or earlier, to access the VMFS2 datastore and perform the VMFS2 to VMFS3 upgrade.

Prerequisites

- Commit or discard any changes to virtual disks in the VMFS2 datastore that you plan to upgrade.
- Back up the VMFS2 datastore.
- Be sure that no powered on virtual machines are using the VMFS2 datastore.
- Be sure that no other ESXi host is accessing the VMFS2 datastore.
- To upgrade the VMFS2 file system, its file block size must not exceed 8MB.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage**.
- 3 Select the datastore that uses the VMFS2 format.
- 4 Click **Upgrade to VMFS3**.
- 5 Perform a rescan on all hosts that see the datastore.

What to do next

After you upgrade your VMFS2 datastore to VMFS3, the datastore becomes available on the ESXi 5.x host. You can now use the ESXi 5.x host to complete the process of upgrading to VMFS5.

Upgrade VMFS3 Datastores to VMFS5 in the vSphere Client

VMFS5 is a new version of the VMware cluster file system that provides performance and scalability improvements.

Prerequisites

- If you use a VMFS2 datastore, you must first upgrade it to VMFS3. Follow the instructions in [“Upgrade VMFS2 Datastores to VMFS3,”](#) on page 155.
- All hosts accessing the datastore must support VMFS5.
- Verify that the volume to be upgraded has at least 2MB of free blocks available and 1 free file descriptor.

Procedure

- 1 Log in to the vSphere Client, and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage**.
- 3 Select the VMFS3 datastore.
- 4 Click **Upgrade to VMFS5**.
A warning message about host version support appears.
- 5 Click **OK** to start the upgrade.
The task Upgrade VMFS appears in the **Recent Tasks** list.
- 6 Perform a rescan on all hosts that are associated with the datastore.

Increase VMFS Datastore Capacity in the vSphere Client

When you need to create virtual machines on a datastore, or when the virtual machines running on a datastore require more space, you can dynamically increase the capacity of a VMFS datastore.

Use one of the following methods to increase a VMFS datastore:

- Add a new extent. An extent is a partition on a storage device. You can add up to 32 extents of the same storage type to an existing VMFS datastore. The spanned VMFS datastore can use any or all of its extents at any time. It does not need to fill up a particular extent before using the next one.
- Grow an extent in an existing VMFS datastore, so that it fills the available adjacent capacity. Only extents with free space immediately after them are expandable.

NOTE If a shared datastore has powered on virtual machines and becomes 100% full, you can increase the datastore's capacity only from the host with which the powered on virtual machines are registered.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

- 1 Log in to the vSphere Client and select a host from the Inventory panel.
- 2 Click the **Configuration** tab and click **Storage**.
- 3 From the Datastores view, select the datastore to increase and click **Properties**.

- 4 Click **Increase**.
- 5 Select a device from the list of storage devices and click **Next**.

Option	Description
To add a new extent	Select the device for which the Expandable column reads NO.
To expand an existing extent	Select the device for which the Expandable column reads YES

- 6 Review the **Current Disk Layout** to see the available configurations and click **Next**.
- 7 Select a configuration option from the bottom panel.

Depending on the current layout of the disk and on your previous selections, the options you see might vary.

Option	Description
Use free space to add new extent	Adds the free space on this disk as a new extent.
Use free space to expand existing extent	Expands an existing extent to a required capacity.
Use free space	Deploys an extent in the remaining free space of the disk. This option is available only when you are adding an extent.
Use all available partitions	Dedicates the entire disk to a single extent. This option is available only when you are adding an extent and when the disk you are formatting is not blank. The disk is reformatted, and the datastores and any data that it contains are erased.

- 8 Set the capacity for the extent.
The minimum extent size is 1.3GB. By default, the entire free space on the storage device is available.
- 9 Click **Next**.
- 10 Review the proposed layout and the new configuration of your datastore, and click **Finish**.

What to do next

After you grow an extent in a shared VMFS datastore, refresh the datastore on each host that can access this datastore, so that the vSphere Client can display the correct datastore capacity for all hosts.

Rename VMFS or NFS Datastores in the vSphere Client

You can change the name of an existing datastore.

Procedure

- 1 Display the datastores.
- 2 Right-click the datastore to rename and select **Rename**.
- 3 Type a new datastore name.

If you use the vCenter Server system to manage your hosts, the new name appears on all hosts that have access to the datastore.

Group VMFS or NFS Datastores in the vSphere Client

If you use the vCenter Server system to manage your hosts, group datastores into folders. This allows you to organize your datastores according to business practices and to assign the same permissions and alarms on the datastores in the group at one time.

Procedure

- 1 Log in to the vSphere Client.
- 2 If necessary, create the datastores.
- 3 In the Inventory panel, choose **Datastores**.
- 4 Select the datacenter containing the datastores to group.
- 5 In the shortcut menu, click the **New Folder** icon.
- 6 Give the folder a descriptive name.
- 7 Click and drag each datastore onto the folder.

Delete VMFS Datastores in the vSphere Client

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

NOTE The datastore delete operation permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

Prerequisites

- Remove all virtual machines from the datastore.
- Make sure that no other host is accessing the datastore.

Procedure

- 1 Display the datastores.
- 2 Right-click the datastore to delete and click **Delete**.
- 3 Confirm that you want to delete the datastore.

Create a Diagnostic Partition in the vSphere Client

You can create a diagnostic partition for your host.

Procedure

- 1 Log in to the vSphere Client and select the host from the Inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Datastores** and click **Add Storage**.
- 4 Select **Diagnostic** and click **Next**.

If you do not see **Diagnostic** as an option, the host already has a diagnostic partition.

- 5 Specify the type of diagnostic partition.

Option	Description
Private Local	Creates the diagnostic partition on a local disk. This partition stores fault information only for your host.
Private SAN Storage	Creates the diagnostic partition on a non-shared SAN LUN. This partition stores fault information only for your host.
Shared SAN Storage	Creates the diagnostic partition on a shared SAN LUN. This partition is accessed by multiple hosts and can store fault information for more than one host.

- 6 Click **Next**.
- 7 Select the device to use for the diagnostic partition and click **Next**.
- 8 Review the partition configuration information and click **Finish**.

Raw Device Mapping

Raw device mapping (RDM) provides a mechanism for a virtual machine to have direct access to a LUN on the physical storage subsystem (Fibre Channel or iSCSI only).

The following topics contain information about RDMs and provide instructions on how to create and manage RDMs.

Create Virtual Machines with RDMs

When you give your virtual machine direct access to a raw SAN LUN, you create a mapping file (RDM) that resides on a VMFS datastore and points to the LUN. Although the mapping file has the same .vmdk extension as a regular virtual disk file, the RDM file contains only mapping information. The actual virtual disk data is stored directly on the LUN.

You can create the RDM as an initial disk for a new virtual machine or add it to an existing virtual machine. When creating the RDM, you specify the LUN to be mapped and the datastore on which to put the RDM.

Procedure

- 1 Follow all steps required to create a custom virtual machine.
- 2 In the Select a Disk page, select **Raw Device Mapping**, and click **Next**.
- 3 From the list of SAN disks or LUNs, select a raw LUN for your virtual machine to access directly.
- 4 Select a datastore for the RDM mapping file.

You can place the RDM file on the same datastore where your virtual machine configuration file resides, or select a different datastore.

NOTE To use vMotion for virtual machines with enabled NPIV, make sure that the RDM files of the virtual machines are located on the same datastore. You cannot perform Storage vMotion when NPIV is enabled.

- 5 Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, powered on virtual machines that use RDMs configured for physical compatibility cannot be migrated if the migration involves copying the disk. Such virtual machines cannot be cloned or cloned to a template either.
Virtual	Allows the RDM to behave as if it were a virtual disk, so you can use such features as snapshotting, cloning, and so on.

- 6 Select a virtual device node.
- 7 If you select Independent mode, choose one of the following.

Option	Description
Persistent	Changes are immediately and permanently written to the disk.
Nonpersistent	Changes to the disk are discarded when you power off or revert to the snapshot.

- 8 Click **Next**.
- 9 In the Ready to Complete New Virtual Machine page, review your selections.
- 10 Click **Finish** to complete your virtual machine.

Manage Paths for a Mapped Raw LUN

You can manage paths for mapped raw LUNs.

Procedure

- 1 Log in as administrator or as the owner of the virtual machine to which the mapped disk belongs.
- 2 Select the virtual machine from the Inventory panel.
- 3 On the **Summary** tab, click **Edit Settings**.
- 4 On the **Hardware** tab, select **Hard Disk**, then click **Manage Paths**.
- 5 Use the Manage Paths dialog box to enable or disable your paths, set multipathing policy, and specify the preferred path.

For information on managing paths, see [“Understanding Multipathing and Failover,”](#) on page 160.

Understanding Multipathing and Failover

To maintain a constant connection between a host and its storage, ESXi supports multipathing. Multipathing is a technique that lets you use more than one physical path that transfers data between the host and an external storage device.

In case of a failure of any element in the SAN network, such as an adapter, switch, or cable, ESXi can switch to another physical path, which does not use the failed component. This process of path switching to avoid failed components is known as path failover.

In addition to path failover, multipathing provides load balancing. Load balancing is the process of distributing I/O loads across multiple physical paths. Load balancing reduces or removes potential bottlenecks.

Note Virtual machine I/O might be delayed for up to sixty seconds while path failover takes place. These delays allow the SAN to stabilize its configuration after topology changes. In general, the I/O delays might be longer on active-passive arrays and shorter on active-active arrays.

Path Scanning and Claiming

When you start your ESXi host or rescan your storage adapter, the host discovers all physical paths to storage devices available to the host. Based on a set of claim rules, the host determines which multipathing plug-in (MPP) should claim the paths to a particular device and become responsible for managing the multipathing support for the device.

By default, the host performs a periodic path evaluation every 5 minutes causing any unclaimed paths to be claimed by the appropriate MPP.

The claim rules are numbered. For each physical path, the host runs through the claim rules starting with the lowest number first. The attributes of the physical path are compared to the path specification in the claim rule. If there is a match, the host assigns the MPP specified in the claim rule to manage the physical path. This continues until all physical paths are claimed by corresponding MPPs, either third-party multipathing plug-ins or the native multipathing plug-in (NMP).

For the paths managed by the NMP module, a second set of claim rules is applied. These rules determine which Storage Array Type Plug-In (SATP) should be used to manage the paths for a specific array type, and which Path Selection Plug-In (PSP) is to be used for each storage device.

Use the vSphere Client to view which SATP and PSP the host is using for a specific storage device and the status of all available paths for this storage device. If needed, you can change the default VMware PSP using the client. To change the default SATP, you need to modify claim rules using the vSphere CLI.

You can find some information about modifying claim rules in the *vSphere Storage* documentation.

For more information about the commands available to manage PSA, see *Getting Started with vSphere Command-Line Interfaces*.

For a complete list of storage arrays and corresponding SATPs and PSPs, see the SAN Array Model Reference section of the *vSphere Compatibility Guide*.

View Datastore Paths in the vSphere Client

Use the vSphere Client to review the paths that connect to storage devices the datastores are deployed on.

Procedure

- 1 Log in to the vSphere Client and select a host from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Datastores** under View.
- 4 From the list of configured datastores, select the datastore whose paths you want to view, and click **Properties**.
- 5 Under Extents, select the storage device whose paths you want to view and click **Manage Paths**.
- 6 In the Paths panel, select the path to view.
The panel underneath displays the path's name. The name includes parameters describing the path: adapter ID, target ID, and device ID.
- 7 (Optional) To extract the path's parameters, right-click the path and select **Copy path to clipboard**.

View Storage Device Paths in the vSphere Client

Use the vSphere Client to view which SATP and PSP the host uses for a specific storage device and the status of all available paths for this storage device.

Procedure

- 1 Log in to the vSphere Client and select a server from the inventory panel.
- 2 Click the **Configuration** tab and click **Storage** in the Hardware panel.
- 3 Click **Devices** under View.
- 4 Select the storage device whose paths you want to view and click **Manage Paths**.
- 5 In the Paths panel, select the path to view.

The panel underneath displays the path's name. The name includes parameters describing the path: adapter ID, target ID, and device ID.

- 6 (Optional) To extract the path's parameters, right-click the path and select **Copy path to clipboard**.

Change the Path Selection Policy in the vSphere Client

Generally, you do not have to change the default multipathing settings your host uses for a specific storage device. However, if you want to make any changes, you can use the Manage Paths dialog box to modify a path selection policy and specify the preferred path for the Fixed policy.

Procedure

- 1 Open the Manage Paths dialog box either from the Datastores or Devices view.
- 2 Select a path selection policy.

By default, VMware supports the following path selection policies. If you have a third-party PSP installed on your host, its policy also appears on the list.

- Fixed (VMware)
- Most Recently Used (VMware)
- Round Robin (VMware)

- 3 For the fixed policy, specify the preferred path by right-clicking the path you want to assign as the preferred path, and selecting **Preferred**.
- 4 Click **OK** to save your settings and exit the dialog box.

Disable Paths in the vSphere Client

You can temporarily disable paths for maintenance or other reasons. You can do so using the vSphere Client.

Procedure

- 1 Open the Manage Paths dialog box either from the Datastores or Devices view.
- 2 In the Paths panel, right-click the path to disable, and select **Disable**.
- 3 Click **OK** to save your settings and exit the dialog box.

You can also disable a path from the adapter's Paths view by right-clicking the path in the list and selecting **Disable**.

Storage Hardware Acceleration

The hardware acceleration functionality enables the ESXi host to integrate with compliant storage arrays and offload specific virtual machine and storage management operations to storage hardware. With the storage hardware assistance, your host performs these operations faster and consumes less CPU, memory, and storage fabric bandwidth.

The hardware acceleration is supported by block storage devices, Fibre Channel and iSCSI, and NAS devices.

For additional details, see the VMware knowledge base article at <http://kb.vmware.com/kb/1021976>.

Disable Hardware Acceleration for Block Storage Devices

On your host, the hardware acceleration for block storage devices is enabled by default. You can use the vSphere Client advanced settings to disable the hardware acceleration operations.

As with any advanced settings, before you disable the hardware acceleration, consult with the VMware support team.

Procedure

- 1 In the vSphere Client inventory panel, select the host.
- 2 Click the **Configuration** tab, and click **Advanced Settings** under **Software**.
- 3 Change the value for any of the options to 0 (disabled):
 - VMFS3.HardwareAcceleratedLocking
 - DataMover.HardwareAcceleratedMove
 - DataMover.HardwareAcceleratedInit

Storage Thin Provisioning

With ESXi, you can use two models of thin provisioning, array-level and virtual disk-level.

Thin provisioning is a method that optimizes storage utilization by allocating storage space in a flexible on-demand manner. Thin provisioning contrasts with the traditional model, called thick provisioning. With thick provisioning, large amount of storage space is provided in advance in anticipation of future storage needs. However, the space might remain unused causing underutilization of storage capacity.

The VMware thin provisioning features help you eliminate storage underutilization problems at the datastore and storage array level.

Create Thin Provisioned Virtual Disks

When you need to save storage space, you can create a virtual disk in thin provisioned format. The thin provisioned virtual disk starts small and grows as more disk space is required.

This procedure assumes that you are creating a typical or custom virtual machine using the New Virtual Machine wizard.

Prerequisites

You can create thin disks only on the datastores that support disk-level thin provisioning.

Procedure

- ◆ In the Create a Disk dialog box, select **Thin Provision**.

A virtual disk in thin format is created.

What to do next

If you created a virtual disk in the thin format, you can later inflate it to its full size.

View Virtual Machine Storage Resources

You can view how datastore storage space is allocated for your virtual machines.

Procedure

- 1 Select the virtual machine in the inventory.
- 2 Click the **Summary** tab.
- 3 Review the space allocation information in the Resources section.
 - **Provisioned Storage** – Shows datastore space allocated to the virtual machine. The entire space might not be used by the virtual machine if it has disks in thin provisioned format. Other virtual machines can occupy any unused space.
 - **Not-shared Storage** – Shows datastore space occupied by the virtual machine and not shared with any other virtual machines.
 - **Used Storage** – Shows datastore space actually occupied by virtual machine files, including configuration and log files, snapshots, virtual disks, and so on. When the virtual machine is running, the used storage space also includes swap files.

Determine the Disk Format of a Virtual Machine

You can determine whether your virtual disk is in thick or thin format.

Procedure

- 1 Select the virtual machine in the inventory.
- 2 Click **Edit Settings** to display the Virtual Machine Properties dialog box.
- 3 Click the **Hardware** tab and select the appropriate hard disk in the Hardware list.
The Disk Provisioning section on the right shows the type of your virtual disk.
- 4 Click **OK**.

What to do next

If your virtual disk is in the thin format, you can inflate it to its full size.

Inflate Thin Virtual Disks

If you created a virtual disk in the thin provision format, you can inflate it to its full size.

This procedure converts a thin disk to a virtual disk in thick provision format.

Procedure

- 1 Select the virtual machine in the inventory.
- 2 Click the **Summary** tab and, under Resources, double-click the datastore for the virtual machine to open the Datastore Browser dialog box.
- 3 Click the virtual machine folder to find the virtual disk file you want to convert. The file has the `.vmdk` extension.
- 4 Right-click the virtual disk file and select **Inflate**.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Resource Management for Single Hosts

14

When you connect the vSphere Client directly to a host, you have access to a limited number of resource management settings, including hyperthreading settings, power management configuration, and swapfile properties.

This chapter includes the following topics:

- [“Configuring Resource Allocation Settings,”](#) on page 167
- [“Administering CPU Resources,”](#) on page 168
- [“Administering Memory Resources,”](#) on page 171
- [“Using NUMA Systems with ESXi,”](#) on page 174
- [“Advanced Attributes,”](#) on page 175

Configuring Resource Allocation Settings

When available resource capacity does not meet the demands of the resource consumers (and virtualization overhead), administrators might need to customize the amount of resources that are allocated to virtual machines or to the resource pools in which they reside.

Use the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine. In particular, administrators have several options for allocating resources.

- Reserve the physical resources of the host or cluster.
- Ensure that a certain amount of memory for a virtual machine is provided by the physical memory of the ESXi machine.
- Guarantee that a particular virtual machine is always allocated a higher percentage of the physical resources than other virtual machines.
- Set an upper bound on the resources that can be allocated to a virtual machine.

Edit System Resource Allocation

Use the Edit System Resource Allocation dialog box to change allocations for memory and CPU resources.

Prerequisites

Required privilege: **Host.Configuration.System Resource Settings**

Procedure

- 1 Click the **Inventory** button in the navigation bar, expand the inventory as needed, and click the appropriate managed host.

- 2 Click the **Configuration** tab to display configuration information for the host.
- 3 Click **System Resource Allocation**.
- 4 Select whether to use **Simple** or **Advanced** resource allocation.

Option	Description
Simple	The CPU and Memory resource settings are applied to the host as a unit.
Advanced	Allows you to edit the CPU and Memory resources allocated to specific host functions or processes. Select a specific system resource pool to edit.

- 5 Click **Edit Settings**.
- 6 Edit the CPU Resources.

Option	Description
Shares	CPU shares for this resource pool with respect to the parent's total. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Guaranteed CPU allocation for this resource pool. Select Expandable Reservation to specify that more than the specified reservation is allocated if resources are available in a parent.
Limit	Upper limit for this resource pool's CPU allocation. Select Unlimited to specify no upper limit.

- 7 Edit the Memory Resources.

Option	Description
Shares	Memory shares for this resource pool with respect to the parent's total. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Guaranteed memory allocation for this resource pool. Select Expandable Reservation to specify that more than the specified reservation is allocated if resources are available in a parent.
Limit	Upper limit for this resource pool's memory allocation. Select Unlimited to specify no upper limit.

- 8 Click **OK**.

Administering CPU Resources

You can configure virtual machines with one or more virtual processors, each with its own set of registers and control structures.

When a virtual machine is scheduled, its virtual processors are scheduled to run on physical processors. The VMkernel Resource Manager schedules the virtual CPUs on physical CPUs, thereby managing the virtual machine's access to physical CPU resources. ESXi supports virtual machines with up to 64 virtual CPUs.

View Processor Information

You can access information about current CPU configuration through the vSphere Client or using the vSphere SDK.

Procedure

- 1 In the vSphere Client, select the host and click the **Configuration** tab.
- 2 Select **Processors**.

You can view the information about the number and type of physical processors and the number of logical processors.

NOTE In hyperthreaded systems, each hardware thread is a logical processor. For example, a dual-core processor with hyperthreading enabled has two cores and four logical processors.

- 3 (Optional) You can also disable or enable hyperthreading by clicking **Properties**.

Enable Hyperthreading

To enable hyperthreading, you must first enable it in your system's BIOS settings and then turn it on in the vSphere Client. Hyperthreading is enabled by default.

Consult your system documentation to determine whether your CPU supports hyperthreading.

Procedure

- 1 Ensure that your system supports hyperthreading technology.
- 2 Enable hyperthreading in the system BIOS.
Some manufacturers label this option **Logical Processor**, while others call it **Enable Hyperthreading**.
- 3 Make sure that you turn on hyperthreading for the ESXi host.
 - a In the vSphere Client, select the host and click the **Configuration** tab.
 - b Select **Processors** and click **Properties**.
 - c In the dialog box, you can view hyperthreading status and turn hyperthreading off or on (default).

Hyperthreading is enabled.

Set Hyperthreading Sharing Options for a Virtual Machine

You can specify how the virtual CPUs of a virtual machine can share physical cores on a hyperthreaded system.

Two virtual CPUs share a core if they are running on logical CPUs of the core at the same time. You can set this for individual virtual machines.

Procedure

- 1 In the vSphere Client inventory panel, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **Resources** tab, and click **Advanced CPU**.
- 3 Select a hyperthreading mode for this virtual machine from the **Mode** drop-down menu.

Assign a Virtual Machine to a Specific Processor

Using CPU affinity, you can assign a virtual machine to a specific processor. This allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

Procedure

- 1 In the vSphere Client inventory panel, select a virtual machine and select **Edit Settings**.
- 2 Select the **Resources** tab and select **Advanced CPU**.
- 3 Click the **Run on processor(s)** button.
- 4 Select the processors where you want the virtual machine to run and click **OK**.

Select a CPU Power Management Policy

You set the CPU power management policy for a host using the vSphere Client.

Prerequisites

Verify that the BIOS settings on the host system allow the operating system to control power management (for example, **OS Controlled**).

NOTE Some systems have Processor Clocking Control (PCC) technology, which allows ESXi to manage power on the host system even if the host BIOS settings do not specify OS Controlled mode. With this technology, ESXi does not manage P-states directly. Instead, the host cooperates with the BIOS to determine the processor clock rate. HP systems that support this technology have a BIOS setting called Cooperative Power Management that is enabled by default.

If the host hardware does not allow the operating system to manage power, only the Not Supported policy is available. (On some systems, only the High Performance policy is available.)

Procedure

- 1 In the vSphere Client inventory panel, select a host and click the **Configuration** tab.
- 2 Under Hardware, select **Power Management** and select **Properties**.
- 3 Select a power management policy for the host and click **OK**.

The policy selection is saved in the host configuration and can be used again at boot time. You can change it at any time, and it does not require a server reboot.

Configure Custom Policy Parameters for Host Power Management

When you use the Custom policy for host power management, ESXi bases its power management policy on the values of several advanced configuration parameters.

Prerequisites

Select **Custom** for the power management policy, as described in [“Select a CPU Power Management Policy,”](#) on page 170.

Procedure

- 1 In the vSphere Client inventory, select the host and click the **Configuration** tab.
- 2 Under Software, select **Advanced Settings**.
- 3 Click **Power** in the left pane.

- 4 In the right pane, you can edit the power management parameters that affect the Custom policy.

Power management parameters that affect the Custom policy have descriptions that begin with **In Custom policy**. All other power parameters affect all power management policies.

NOTE The default values of power management parameters match the Balanced policy.

Parameter	Description
Power.UsePStates	Use ACPI P-states to save power when the processor is busy.
Power.MaxCpuLoad	Use P-states to save power on a CPU only when the CPU is busy for less than the given percentage of real time.
Power.MinFreqPct	Do not use any P-states slower than the given percentage of full CPU speed.
Power.UseStallCtr	Use a deeper P-state when the processor is frequently stalled waiting for events such as cache misses.
Power.TimerHz	Controls how many times per second ESXi reevaluates which P-state each CPU should be in.
Power.UseCStates	Use deep ACPI C-states (C2 or below) when the processor is idle.
Power.CStateMaxLatency	Do not use C-states whose latency is greater than this value.
Power.CStateResidencyCoef	When a CPU becomes idle, choose the deepest C-state whose latency multiplied by this value is less than the host's prediction of how long the CPU will remain idle. Larger values make ESXi more conservative about using deep C-states, while smaller values are more aggressive.
Power.CStatePredictionCoef	A parameter in the ESXi algorithm for predicting how long a CPU that becomes idle will remain idle. Changing this value is not recommended.
Power.PerfBias	Performance Energy Bias Hint (Intel-only). Sets an MSR on Intel processors to an Intel-recommended value. Intel recommends 0 for high performance, 6 for balanced, and 15 for low power. Other values are undefined.

Administering Memory Resources

Using the vSphere Client you can view information about and make changes to memory allocation settings. To administer your memory resources effectively, you must also be familiar with memory overhead, idle memory tax, and how ESXi hosts reclaim memory.

When administering memory resources, you can specify memory allocation. If you do not customize memory allocation, the ESXi host uses defaults that work well in most situations.

You can specify memory allocation in several ways.

- Use the attributes and special features available through the vSphere Client. The vSphere Client user interface allows you to connect to the ESXi host or vCenter Server system.
- Use advanced settings.
- Use the vSphere SDK for scripted memory allocation.

Enable Host-Local Swap for a Standalone Host

Host-local swap allows you to specify a datastore stored locally on the host as the swap file location. You can enable host-local swap for a standalone host.

Procedure

- 1 In the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, select **Virtual Machine Swapfile Location**.

- 4 Select **Store the swapfile in the swapfile datastore**.
- 5 Select a local datastore from the list and click **OK**.

Host-local swap is now enabled for the standalone host.

Configure Virtual Machine Swapfile Properties for the Host

Configure a swapfile location for the host to determine the default location for virtual machine swapfiles.

By default, swapfiles for a virtual machine are located on a VMFS3 datastore in the folder that contains the other virtual machine files. However, you can configure your host to place virtual machine swapfiles on an alternative datastore.

You can use this option to place virtual machine swapfiles on lower-cost or higher-performance storage. You can also override this host-level setting for individual virtual machines.

Setting an alternative swapfile location might cause migrations with vMotion to complete more slowly. For best vMotion performance, store virtual machine swapfiles in the same directory as the virtual machine.

If vCenter Server manages your host, you cannot change the swapfile location if you connect directly to the host by using the vSphere Client. You must connect the vSphere Client to the vCenter Server system.

Prerequisites

Required privilege: **Host machine.Configuration.Storage partition configuration**

Procedure

- 1 In the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Click the **Virtual Machine Swapfile Location** link.

The **Configuration** tab displays the selected swapfile location. If configuration of the swapfile location is not supported on the selected host, the tab indicates that the feature is not supported.

If the host is part of a cluster, and the cluster settings specify that swapfiles are to be stored in the same directory as the virtual machine, you cannot edit the swapfile location from the host configuration tab. To change the swapfile location for such a host, use the Cluster Settings dialog box.

- 4 Click **Edit**.
- 5 Select either **Store the swapfile in the same directory as the virtual machine** or **Store the swapfile in a swapfile datastore selected below**.
If you select **Store the swapfile in a swapfile datastore selected below**, select a datastore from the list.
- 6 Click **OK**.

The virtual machine swapfile is stored in the location you selected.

Configure the Host Cache

You can change the percentage of space allocated for host cache or disable the host's ability to swap to host cache.

Prerequisites

You must have an SSD-backed datastore in your inventory.

Procedure

- 1 In the vSphere Client, select the host in the inventory.

- 2 Click the **Configuration** tab.
- 3 Under Software, click **Host Cache Configuration**.
- 4 Select the datastore in the list and click **Properties**.
- 5 Select a size for the host cache allocation on the drive.
- 6 To disable the ability for the host to swap to host cache on a per-datastore basis, deselect the **Allocate space for host cache** check box.
- 7 Click **OK**.

Enable or Disable the Memory Compression Cache

Memory compression is enabled by default. You can use the Advanced Settings dialog box in the vSphere Client to enable or disable memory compression for a host.

Procedure

- 1 In the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, select **Advanced Settings**.
- 4 In the left pane, select **Mem** and locate Mem.MemZipEnable.
- 5 Enter 1 to enable or enter 0 to disable the memory compression cache.
- 6 Click **OK**.

Set the Maximum Size of the Memory Compression Cache

You can set the maximum size of the memory compression cache for the host's virtual machines.

You set the size of the compression cache as a percentage of the memory size of the virtual machine. For example, if you enter 20 and a virtual machine's memory size is 1000 MB, ESXi can use up to 200MB of host memory to store the compressed pages of the virtual machine.

If you do not set the size of the compression cache, ESXi uses the default value of 10 percent.

Procedure

- 1 In the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, select **Advanced Settings**.
- 4 In the left pane, select **Mem** and locate Mem.MemZipMaxPct.
The value of this attribute determines the maximum size of the compression cache for the virtual machine.
- 5 Enter the maximum size for the compression cache.
The value is a percentage of the size of the virtual machine and must be between 5 and 100 percent.
- 6 Click **OK**.

Using NUMA Systems with ESXi

ESXi supports memory access optimization for Intel and AMD Opteron processors in server architectures that support NUMA (non-uniform memory access).

After you understand how ESXi NUMA scheduling is performed and how the VMware NUMA algorithms work, you can specify NUMA controls to optimize the performance of your virtual machines.

Associate Virtual Machines with Specific Processors

You might be able to improve the performance of the applications on a virtual machine by pinning its virtual CPUs to fixed processors. This allows you to prevent the virtual CPUs from migrating across NUMA nodes.

Procedure

- 1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.
- 2 Select the **Resources** tab, and select **Advanced CPU**.
- 3 In the Scheduling Affinity panel, set the CPU affinity to the preferred processors.

NOTE You must manually select the boxes for all processors in the NUMA node. CPU affinity is specified on a per-processor, not on a per-node, basis.

Associate Memory Allocations with Specific NUMA Nodes Using Memory Affinity

You can specify that all future memory allocations on a virtual machine use pages associated with specific NUMA nodes (also known as manual memory affinity).

NOTE Specify nodes to be used for future memory allocations only if you have also specified CPU affinity. If you make manual changes only to the memory affinity settings, automatic NUMA rebalancing does not work properly.

Procedure

- 1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.
- 2 Select the **Resources** tab, and select **Memory**.
- 3 In the NUMA Memory Affinity panel, set memory affinity.

Example: Binding a Virtual Machine to a Single NUMA Node

The following example illustrates manually binding the last four physical CPUs to a single NUMA node for a two-way virtual machine on an eight-way server.

The CPUs (for example, 4, 5, 6, and 7) are the physical CPU numbers.

- 1 In the vSphere Client inventory panel, select the virtual machine and select **Edit Settings**.
- 2 Select **Options** and click **Advanced**.
- 3 Click the **Configuration Parameters** button.
- 4 In the vSphere Client, turn on CPU affinity for processors 4, 5, 6, and 7.

Then, you want this virtual machine to run only on node 1.

- 1 In the vSphere Client inventory panel, select the virtual machine and select **Edit Settings**.
- 2 Select **Options** and click **Advanced**.

- 3 Click the **Configuration Parameters** button.
- 4 In the vSphere Client, set memory affinity for the NUMA node to 1.

Completing these two tasks ensures that the virtual machine runs only on NUMA node 1 and, when possible, allocates memory from the same node.

Associate Virtual Machines with Specified NUMA Nodes

When you associate a NUMA node with a virtual machine to specify NUMA node affinity, you constrain the set of NUMA nodes on which NUMA can schedule a virtual machine's virtual CPU and memory.

NOTE When you constrain NUMA node affinities, you might interfere with the ability of the ESXi NUMA scheduler to rebalance virtual machines across NUMA nodes for fairness. Specify NUMA node affinity only after you consider the rebalancing issues.

Procedure

- 1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **Options** tab.
- 3 Select **Advanced > General**.
- 4 Click **Configuration Parameters**.
- 5 Click **Add Row** to add a new option.
- 6 In the Name column, enter **numa.nodeAffinity**.
- 7 In the Value column, enter the NUMA nodes where the virtual machine can be scheduled.

Use a comma-separated list for multiple nodes. For example, enter **0,1** to constrain the virtual machine resource scheduling to NUMA nodes 0 and 1.

- 8 Click **OK**.
- 9 Click **OK** to close the Virtual Machine Properties dialog box.

Advanced Attributes

You can set advanced attributes for hosts or individual virtual machines to help you customize resource management.

In most cases, adjusting the basic resource allocation settings (reservation, limit, shares) or accepting default settings results in appropriate resource allocation. However, you can use advanced attributes to customize resource management for a host or a specific virtual machine.

Set Advanced Host Attributes

You can set advanced attributes for a host.



CAUTION Changing advanced options is considered unsupported unless VMware technical support or a KB article instruct you to do so. In all other cases, changing these options is considered unsupported. In most cases, the default settings produce the optimum result.

Procedure

- 1 In the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under **Software**, click **Advanced Settings**.

- 4 In the Advanced Settings dialog box, select the appropriate item (for example, **CPU** or **Mem**).
- 5 Locate the attribute in the right panel and edit the value.
- 6 Click **OK**.

Set Advanced Virtual Machine Attributes

You can set advanced attributes for a virtual machine.

Procedure

- 1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.
- 2 Click **Options** and click **Advanced > General**.
- 3 Click **Configuration Parameters**.
- 4 In the dialog box that appears, click **Add Row** to enter a new parameter and its value.
- 5 Click **OK**.

Monitoring a Single Host with the vSphere Client

15

When you connect to a single host using the vSphere Client, you can monitor the host health status, and view events, system logs, and performance charts.

This chapter includes the following topics:

- [“Monitoring Host Health Status,”](#) on page 177
- [“View Events,”](#) on page 178
- [“View System Logs,”](#) on page 179
- [“View Charts,”](#) on page 179

Monitoring Host Health Status

You can use the vSphere Client or the vSphere Web Client to monitor the state of host hardware components, such as CPU processors, memory, fans, and other components.

The host health monitoring tool allows you to monitor the health of a variety of host hardware components including:

- CPU processors
- Memory
- Fans
- Temperature
- Voltage
- Power
- Network
- Battery
- Storage
- Cable/Interconnect
- Software components
- Watchdog
- Other

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware. SMASH is an industry standard specification providing protocols for managing a variety of systems in the datacenter. For more information, see <http://www.dmtf.org/standards/smash>.

You can monitor a host's health status either by connecting the vSphere Client directly to a host, or by connecting to a vCenter Server system. You can also set alarms to trigger when the host health status changes.

Monitor Health Status When Directly Connected to a Host

When you connect the vSphere Client directly to a host, you can view the health status from the host's **Configuration** tab.

Prerequisites

Required privilege: **Host.Configuration.Advanced Configuration**

Procedure

- 1 Log in to the host using the vSphere Client, and display the inventory.
- 2 Click the **Configuration** tab, and click **Health Status**.

If a component is functioning normally, the status indicator is green. The status indicator changes to yellow or red if a system component violates a performance threshold or is not functioning properly. Generally, a yellow indicator signifies degraded performance. A red indicator signifies that a component stopped operating or exceeded the highest threshold. If the status is blank, then the health monitoring service cannot determine the status of the component.

The **Reading** column displays the current values for the sensors. For instance, the column displays rotations per minute (RPM) for fans and degrees Celsius for temperature.

Reset Hardware Sensors When Directly Connected to a Host

Some host hardware sensors display data that is cumulative over time. You can reset these sensors to clear the data in them and begin collecting new data.

Prerequisites

If you need to preserve sensor data for troubleshooting or other purposes, take a screenshot, export the data, or download a support bundle before resetting sensors.

Procedure

- 1 On the host **Configuration** tab, click **Health Status**.
- 2 Click **Reset Sensors**.

View Events

You can either view all vSphere events or view events associated with a single object. The events list for a selected inventory object includes events associated with child objects.

Prerequisites

Required privilege: **Read-only**

Procedure

- ◆ To see a list of events associated with a selected inventory object and its child objects, select the **Tasks & Events** tab and click **Events**.
 - a Select an event to see event details.
 - b Use the filter controls above the list to filter the list.
 - c Click a column heading to sort the list.

View System Logs

System log entries include such information as who generated the event, when the event was created, and the type of event.

Prerequisites

Connect to an ESX/ESXi host by using the vSphere Client.

Required privilege: **Global. Diagnostics** privilege.

Procedure

- 1 To view system log entries, select **Home > Administration > System Logs**.
- 2 From the drop-down menu, select the log.
- 3 (Optional) Click **Show All** or **Show next # lines** to see additional log entries.
- 4 (Optional) Filter the log entries.
 - a Select **View > Filtering**.
 - b Type the filter criteria in the filter box.

View Charts

You can connect directly to ESX/ESXi hosts and view information about resource usage in line chart form.

Prerequisites

Connect to an ESX/ESXi host by using the vSphere Client.

Procedure

- 1 Select the host in the inventory.
- 2 Click the **Performance** tab.
- 3 Select a resource type from the **Switch to** drop-down menu.
- 4 (Optional) Click **Chart Options** to modify performance charts.

Index

A

- acceleration
 - disabling **109**
 - enabling **109**
- active adapters **127**
- Active Directory **40, 41**
- adapters, Ethernet, *See* network adapters
- adding
 - NFS storage **152**
 - paravirtual SCSI controller **88**
 - SCSI controllers **86**
 - SCSI devices **92**
 - USB controllers **97, 102**
 - USB devices to client computers **102**
- adding a VMkernel network adapter **125**
- Administrator role **38**
- advanced attributes
 - hosts **175**
 - virtual machines **176**
- advanced settings
 - Disk.EnableNaviReg **133**
 - Disk.MaxLUN **150**
- allowed IP addresses, firewall **30**
- AMD Opteron-based systems **174**
- AMD override mask **69**
- assigning license keys **23**
- authentication
 - ESXi **33**
 - ESXi users **33**
 - users **33**
- authentication proxy **40, 41**
- automatic host registration, disabling **133**

B

- BIOS, settings **108**
- boot options
 - changing BIOS settings **108**
 - changing delay **108**

C

- cable/interconnect, health monitoring **177**
- CAM server **41**
- CHAP
 - disabling **148**
 - for discovery targets **147**

- for iSCSI initiators **146**
 - for static targets **147**
- CHAP authentication **146**
- character classes, passwords **35**
- charts, viewing **179**
- claim rules **161**
- client startup options, setting **30**
- configuration file parameters, editing **62**
- configuring
 - dynamic discovery **144**
 - hosts **19**
 - static discovery **145**
- consoles, virtual machines **17**
- controllers
 - paravirtual SCSI **88**
 - SCSI **49**
 - SCSI types **87**
- CPU
 - health monitoring **177**
 - managing allocation **168**
- CPU affinity, NUMA nodes **174**
- CPU resources, editing **167**
- CPUs
 - adding **47**
 - advanced settings **68**
 - configuration **66**
 - defined **64**
 - disabling security **69**
 - enabling CPU/MMU Virtualization **70**
 - hot adding **66**
 - hot plug **65**
 - hyperthreaded core sharing **68**
 - identification mask **69**
 - limits **67**
 - parameters **64**
 - reservation **67**
 - scheduling affinity **69**
 - shares **67**
- creating, virtual machines **43**
- current multipathing state **161**

D

- datastores
 - adding extents **156**
 - configuring on NFS volumes **152**
 - grouping **158**

- increasing capacity **156**
- ISO file **90**
- managing duplicate **153**
- mounting **153**
- NFS **151**
- paths **161**
- renaming **157**
- review properties **130**
- selecting **45**
- VMFS **49, 151**
- debugging and statistics **109**
- dependent iSCSI, networking **138**
- dependent hardware iSCSI
 - and associated NICs **136**
 - configuration workflow **135**
- deploying, OVF templates **55**
- determining which features are licensed **24**
- diagnostic partition, configuring **158**
- direct access **33**
- direct console, redirecting to a serial port **19**
- directory server, viewing **41, 42**
- directory service
 - Active Directory **40**
 - configuring a host **40**
- disabling paths **162**
- discovery
 - address **144**
 - dynamic **144**
 - static **145**
- disk formats
 - thick provisioned **81**
 - thin provisioned **81**
- Disk.EnableNaviReg **133**
- Disk.MaxLUN **150**
- disks
 - format **85, 86, 164**
 - independent **116**
 - inflate **164**
 - limits **84**
 - modes **83**
 - shares **84**
- DVD/CD-ROM, adding **90**
- dynamic discovery, configuring **144**
- dynamic discovery addresses **144**

E

EFI

- changing boot delay **108**
- settings **108**

ESXi

- adding users **33**
- authentication **33**
- rebooting **19**
- shutdown **19**

- syslog service **20**

- users **33**

- events, viewing **178**

- exporting

- host users **35**

- lists **18**

- OVF templates **55, 57**

- virtual machines **57**

- Extensible Firmware Interface, *See* EFI

- extents

- adding to datastore **156**

- growing **156**

F

- failover **160**

- fans, monitoring **177**

- Fibre Channel NPIV settings **80**

- filtering, lists **17**

- firewall settings **30**

- firewalls

- access for management agents **29**

- access for services **29**

- floppy drives

- adding **92**

- configuring **91**

G

- Getting Started tabs

- disabling **16**

- restoring **17**

- guest operating systems

- changing **63**

- selecting **46**

H

- hardware, virtual machine **59**

- hardware acceleration

- about **163**

- enabling **163**

- hardware devices, SCSI controllers **86**

- hardware health, reset sensors **178**

- hardware iSCSI initiators

- configuring **134**

- installing **134**

- setting up discovery addresses **144**

- viewing **134**

- hardware requirements, vSphere Client **11**

- health status, monitoring **178**

- host cache configuration **172**

- host configuration, advanced settings **133**

- host health, reset sensors **178**

- host image profile acceptance level **21**

- host name, configuring **40**

- host networking, viewing **123**

- host power management, custom policy **170**

host power management policies, setting **170**
 host registration, disabling **133**
 host-local swap, standalone host **171**
 hosts

- adding ESXi users **33**
- advanced attributes **175**
- configuring **19**
- ESXi **19**
- hardware monitoring **177**
- health status **178**
- viable for migration **69**
- virtual machine swapfile location **172**

hot add enablement **65, 72**
 hyperthreaded core sharing **68**
 hyperthreading
 disabling **169**
 enabling **169**
 server configuration for **169**
 hyperthreading modes **169**

I

image files, ISO **89, 90**
 independent disks **116**
 independent hardware iSCSI adapters
 change IP address **135**
 change name **135**
 installing, vSphere Client **13**
 installing the vSphere Client **13**
 installing, vSphere Client **11**
 IP addresses, adding allowed **30**
 IP storage port groups, creating **125**
 iSCSI initiators
 configuring advanced parameters **149**
 configuring CHAP **146**
 hardware **134**
 setting up CHAP parameters **146**
 iSCSI networking
 binding adapters **143**
 changing policy **142**
 creating a VMkernel interface **141**
 ISO image files **89, 90**

J

jumbo frames
 enabling for dependent hardware iSCSI **144**
 enabling for software iSCSI **144**
 using with iSCSI **143**

L

license key **23**
 License key **25**
 License management **23**
 licensed features **24**
 licenses, assigning **23**

lists
 exporting **18**
 filtering **17**
 logging, enabling **109**
 logging in, vSphere Client **15**
 logging out, vSphere Client **16**
 logical processors **169**
 logs,system, *See also* troubleshooting
 LUNs, changing number scanned **150**

M

MAC addresses, assigning **74**
 management interface, securing **29**
 management access
 firewalls **29**
 TCP and UDP ports **12**
 managing, virtual machines **111**
 mask values **69**
 memory
 affinity **72**
 allocation **71**
 calculating for video displays **94**
 health monitoring **177**
 hot adding **72**
 managing allocation **171**
 virtual **47**
 memory affinity, NUMA nodes **174**
 memory compression cache
 disabling **173**
 enabling **173**
 set size **173**
 memory resources, editing **167**
 Microsoft .NET Framework **12**
 migration
 cross-host Storage vMotion **81**
 storage **81**
 monitoring, vSphere Client **177**
 multicore CPUs **65**
 multipathing plug-ins, path claiming **161**
 multipathing state **161**
 multiple monitors, selecting **94**

N

network adapters
 viewing **123**
 See also NICs
 network connections, create **140**
 networking **123**
 networks
 connecting **48**
 health monitoring **177**
 New Virtual Machine wizard, opening **43**
 NFS storage, adding **152**
 NIC teaming **127**

- NICs
 - assigning MAC addresses **74**
 - configuring **74**
 - mapping to VMkernel **141**
 - Spanning Tree protocol **48**
- NMP, path claiming **161**
- No Access role **38**
- NPIV
 - assigning WWNs **130**
 - changing WWNs **131**
- NTP **40**
- NUMA
 - CPU affinity **174, 175**
 - memory affinity **175**
- NX flag **69**
- O**
- optical drives
 - connecting to client device **89**
 - connecting to host device **89**
- OVA, selecting, *See also* OVF
- OVF
 - browsing virtual appliance marketplace **57**
 - deploying templates **55**
 - exporting templates **55, 57**
 - folder location for files **57**
- P**
- parallel ports
 - adding **80**
 - changing **79**
- paravirtual SCSI controller **88**
- passphrase **35**
- passwords
 - character classes **35**
 - requirements **35**
- path claiming **161**
- path failover **160**
- path management **160**
- path policies, changing defaults **162**
- paths, disabling **162**
- PCI devices, snapshot support for **93**
- performance charts **179**
- permissions
 - administrator **36**
 - and privileges **36**
 - assigning **37**
 - changing **37**
 - overview **36**
 - removing **37**
 - root user **36**
 - validating **37**
 - vpxuser **36**
- physical compatibility mode **52**
- physical processors **169**
- policies, host power management **170**
- port configuration **126**
- port groups **124**
- ports
 - adding parallel **80**
 - changing parallel **79**
 - changing serial **77**
 - parallel **75**
 - serial **75**
- power, health monitoring **177**
- power off, virtual machines **107**
- power on, virtual machines **107**
- power states, virtual machine **107**
- printing, vSphere Client window **18**
- privileges and permissions **36**
- processors
 - health monitoring **177**
 - See also* CPUs
- PVSCSI, *See also* paravirtual SCSI controller
- R**
- raw device mapping **159**
- raw device mappings **49, 52, 81, 83**
- RDMs, path management **160**
- Read Only role **38**
- requirements for vSphere Client **12**
- rescanning
 - datastores **150**
 - storage adapters **150**
 - storage devices **150**
- reset sensors, host health **178**
- resetting virtual machines **107**
- resignaturing **153**
- resource allocation settings **167**
- resource management
 - customizing **175**
 - hosts **167**
- restart settings, for virtual machines **107**
- resume, virtual machines **107**
- roles
 - Administrator **38**
 - and permissions **38**
 - cloning **38**
 - copy **38**
 - creating **38**
 - default **38**
 - editing **39**
 - No Access **38**
 - Read Only **38**
 - removing **37, 39**
 - renaming **39**
 - security **38**

root login, permissions **36**

S

SAN LUN **52**

SAN LUNs **81, 83**

scanning, changing number **150**

scheduling affinity **69**

scratch partition, enabling **20**

SCSI

bus sharing **87**

changing controller type **87**

controller **86**

controllers, adding **86**

devices, adding **92**

devices, changing **93**

paravirtual controllers **88**

selecting controllers **49**

supported controller types **87**

VMware Paravirtual **49**

SCSI controller

adding **86**

and virtual device nodes **86**

default virtual hard disk assignments **86**

maximum number of **86**

security, permissions **36**

selecting datastores **45**

serial port, redirecting the direct console using
the vSphere Client **19**

serial ports

adding **78**

adding Firewall rule set **76**

changing **77**

conditions for network connections **76**

conditions for physical connections **75**

connection types **75**

server configuration for hyperthreading **169**

service startup

changing policy **30**

setting options **30**

service startup options, setting **30**

services, syslogd **20**

set host to evaluation mode **24**

shares **167**

sharing, disks **51**

shell access, disabling **30**

shutdown, settings for virtual machines **107**

shutdown, settings, for virtual machines **111**

single host management **7**

smart card reader

adding to virtual machines **106**

shared **106**

SMASH **177**

snapshots

about **113**

behavior **113**

child **113**

consolidating **121**

Delete all option **119**

Delete option **119**

deleting **119, 120**

delta disks **113**

exclude virtual disks from **116**

GO to command **119**

hierarchy **113**

memory **115**

parent **113**

quiescing **116**

quiescing virtual machine files **115**

restoring **117, 119**

revert to parent **119**

reverting to **117**

taking **115, 116**

virtual machine activity **115**

virtual machines with dynamic disks **116**

software iSCSI, networking **138**

software FCoE

and VMkernel **132**

activating adapters **133**

software iSCSI adapter

configuring **137**

disabling **138**

software iSCSI initiator, enabling **137**

software iSCSI initiators, setting up discovery
addresses **144**

standard switch **124**

standard switches, port configuration **126**

standby adapters **127**

standby settings, for virtual machines **107**

starting, vSphere Client **15**

startup settings, for virtual machines **111**

static discovery, configuring **145**

static discovery addresses **144**

storage

health monitoring **177**

managing **129**

not-shared **164**

provisioned **164**

used by virtual machines **164**

storage device, renaming **149**

storage adapters

about **135**

rescanning **150**

viewing **130**

- storage controllers
 - limitations for VMware Paravirtual SCSI **88**
 - VMware Paravirtual SCSI **88**
- storage devices
 - displaying for a host **130**
 - displaying for an adapter **130**
 - managing **149**
 - paths **162**
 - rescanning **150**
- storing, device nodes, using nondefault device notes **50**
- support information **23**
- suspending, virtual machines **107**
- swap file location **73**
- swap to SSD **172**
- swapfiles **172**
- syslog **20**
- system resource allocation, editing **167**
- Systems Management Architecture for Server Hardware, *See* SMASH

T

- tabs, Getting Started **16**
- tasks
 - about **27**
 - filtering with keywords **27**
 - viewing recent tasks **27**
- TCP ports **12**
- temperature, monitoring **177**
- templates
 - OVF **57**
 - returning to a host **113**
- thin disks, creating **163**
- thin provisioned disks **85**
- thin provisioning **163**
- Thin Provisioning **50**
- troubleshooting
 - debugging and statistics **109**
 - virtual machine software installation **109**

U

- UDP ports **12**
- updated information **9**
- upgrading
 - virtual machine hardware **60**
 - VMware Tools **63**
- uplink adapters
 - adding **127**
 - duplex **127**
 - speed **127**
- USB controllers
 - adding to virtual machine **97, 102**
 - removing from virtual machine **99, 105**

USB devices

- adding from client computer to VM in the vSphere Client **104**
- adding host device to virtual machine **98**
- adding to client computers **102**
- adding to hosts **96**
- behavior with hot add operations **100**
- cascading hubs **96**
- compound **96**
- connecting to a client computer **101**
- removing from host **100**
- removing from remote client **105**
- removing from virtual machine **99**
- removing remote client device from VM **104**
- setting up on host **96**
- supported devices for Mac OS X guest **100**

USB passthrough

- arbitrator for **95**
- avoiding data loss **100**
- configuring from a client computer to a VM **100**
- configuring from a host to a virtual machine **95**
- controllers for **95, 100**
- devices, *See also* USB devices
- DRS requirements **101**
- features supported with **101**
- user management, ESXi **33**
- users
 - adding to ESXi **33**
 - authentication **33**
 - direct access **33**
 - exporting a user list **35**
 - modifying on hosts **34**
 - removing **37**
 - removing from hosts **35**
 - security **33**
 - viewing user list **35**

V

- vCenter Converter client plug-in **55**
- version, virtual machine **46**
- VI Client **13**
- video cards
 - configuring **94**
 - selecting number of displays **94**
- virtual compatibility mode **52**
- virtual device node **93**
- virtual devices
 - adding USB controller **97, 102**
 - CPU limitations **65**
- virtual disks
 - clustering features **50**

- configuration **82**
- configuring **81**
- creating **50**
- flat format **50**
- formats **81**
- modes **50**
- sharing **51**
- thick format **85**
- thin format **50, 85**
- types **49**
- using nondefault device node **50, 51**
- virtual hardware
 - adding host USB devices to virtual machine **98**
 - adding USB devices **104**
 - CPU advanced settings **68, 69**
 - CPU hyperthreading **68**
 - CPU/MMU enablement **70**
 - CPUs **47**
 - disks **49**
 - hot add enablement **65**
 - hot adding virtual CPUs **66**
 - memory **47**
 - multicore CPUs **65**
 - NICs **48**
 - parallel ports **79, 80**
 - SCSI controllers **49**
 - SCSI devices **92, 93**
 - serial ports **78**
 - video cards **94**
- virtual machine, memory **71**
- Virtual Machine Communication Interface, *See* VMCI, enabling
- virtual machine console **112**
- virtual machine hardware
 - determining version **61**
 - upgrading **60**
 - virtual disks **82**
- virtual machine hardware version **60**
- virtual machine networking **124**
- virtual machines
 - acceleration **109**
 - advanced attributes **176**
 - assigning to a specific processor **170**
 - assigning WWNs to **130**
 - changing name **61**
 - completing **53**
 - configuration file location **62**
 - configuring **59**
 - configuring devices **89**
 - CPU configuration **66**
 - CPU resources **64**
 - creating **43, 44**
 - debugging **109**
 - enabling logging **109**
 - exporting **57**
 - floppy drives **91, 92**
 - guest operating system **63**
 - hard disks **83**
 - hardware **59**
 - hardware version **61**
 - hardware versions **60**
 - hot add enablement **72**
 - managing **111**
 - memory **71**
 - naming **45**
 - network adapter **75**
 - network configuration **74**
 - NIC **75**
 - opening console **112**
 - optical drives **90**
 - power management settings **106**
 - power states **107**
 - remove from a host **112**
 - remove from the datastore **113**
 - resources **59**
 - returning to a host **113**
 - selecting configuration option for creation **44**
 - selecting guest operating systems **46**
 - shutdown settings **111**
 - snapshots **113**
 - startup settings **111**
 - swap file **73**
 - swapfile location **172**
 - upgrading hardware version **60**
 - versions **46**
 - view console **17**
 - Virtual SMP **47**
 - with RDMs **159**
 - See also* templates, clones
 - See also* virtual hardware
- virtual memory
 - allocation **71**
 - configuring **70**
- virtual processors, *See* CPUs
- Virtual Serial Port Concentrator **75, 78**
- Virtual SMP **47**
- VMCI, enabling **93**
- VMFS, resignaturing **153**
- VMFS datastores
 - adding extents **156**
 - changing signatures **154**
 - creating on Fibre Channel storage **151**
 - creating on iSCSI storage **151**

- creating on SCSI disk **151**
- creating on storage device **151**
- deleting **158**
- increasing capacity **156**
- rescanning **150**
- upgrading **155**
- VMFS resignaturing **153**
- VMFS volume **81**
- VMFS2 datastores, upgrading **155**
- VMFS3, upgrading **156**
- VMkernel
 - gateway **126**
 - prefix **126**
 - routing **126**
- VMkernel interfaces **141**
- VMkernel network adapters, adding **125**
- vMotion
 - CD-ROM migration limitation **89**
 - compatibility **69**
- vMotion interfaces, creating **125**
- VMware Paravirtual SCSI controllers **88**
- VMware Tools, upgrading **63**
- vSPC **75, 78**
- vSphere Client
 - about **15**
 - downloading **13**
 - hardware requirements **11**
 - installing **11, 13**
 - logging in **15**
 - logging out **16**
 - printing data **18**
 - requirements **12**
 - starting **15**
 - stop **16**
- vSphere Authentication Proxy **40, 41**
- vSphere CLI **20**
- vSphere standard switch
 - port configuration **126**
 - viewing **123**

W

- watchdog, health monitoring **177**
- World Wide Names, *See* WWNs
- WWNNs **130**
- WWNs
 - assigning to virtual machines **130**
 - changing **131**
- WWPNs **130**