

vSphere Single Host Management - VMware Host Client

Update 2

Modified on 27 APR 2018

VMware vSphere 6.0

VMware ESXi 6.0

VMware Host Client 1.4



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2015 – 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About vSphere Single Host Management - VMware Host Client	5
Updated Information	6
1 VMware Host Client Overview	7
VMware Host Client System Requirements	7
Using the VMware Host Client	8
2 Host Management with the VMware Host Client	10
Managing System Settings in the VMware Host Client	10
Managing Hosts in vCenter Server	18
Reboot or Shut Down an ESXi Host in the VMware Host Client	19
Using the ESXi Shell	20
Place a Host in Maintenance Mode in the VMware Host Client	21
Generate a Support Bundle in the VMware Host Client	21
Monitoring an ESXi Host in the VMware Host Client	22
Lockdown Mode	24
Administering CPU Resources by Using the VMware Host Client	26
3 Virtual Machine Management with the VMware Host Client	28
Creating a Virtual Machine in the VMware Host Client	28
Deploying a Virtual Machine from an OVF or OVA File in the VMware Host Client	33
Registering an Existing Virtual Machine in the VMware Host Client	35
Using Consoles in the VMware Host Client	36
Managing a Guest Operating System in the VMware Host Client	38
Configuring a Virtual Machine in the VMware Host Client	42
Managing Virtual Machines in the VMware Host Client	71
Monitoring a Virtual Machine in the VMware Host Client	83
4 Managing Storage in the VMware Host Client	86
Working with Datastores in the VMware Host Client	86
View Storage Adapters in the VMware Host Client	101
Managing Storage Devices in the VMware Host Client	101
Monitoring Storage in the VMware Host Client	102
Performing Storage Refresh and Rescan Operations in the VMware Host Client	103
5 Networking in the VMware Host Client	105
Performing Port Group Tasks in the VMware Host Client	105

Managing Virtual Switches in the VMware Host Client	107
Managing Physical Network Adapters in the VMware Host Client	109
Managing VMkernel Network Adapters in the VMware Host Client	109
View TCP/IP Stack Configuration on a Host in the VMware Host Client	112
Change the Configuration of a TCP/IP Stack on a Host in the VMware Host Client	113
Configuring ESXi Firewall in the VMware Host Client	113
Monitoring Networking Events and Tasks in the VMware Host Client	115

About vSphere Single Host Management - VMware Host Client

vSphere Single Host Management - VMware Host Client provides information about managing single hosts with the VMware Host Client.

The VMware Host Client can be utilized to conduct emergency management when vCenter Server is unavailable. You can use the VMware Host Client to perform administrative tasks and basic troubleshooting tasks, as well as advanced administrative tasks.

Intended Audience

This information is intended for anyone who wants to use the VMware Host Client to manage single ESXi hosts. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

Updated Information

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

This table provides the update history of the *vSphere Single Host Management - VMware Host Client*.

Revision	Description
27 APR 2018	Updated the note about taking snapshots in Take a Snapshot in the VMware Host Client .
15 MAR 2016	Initial release.

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts.

You can use the VMware Host Client to perform administrative and basic troubleshooting tasks, as well as advanced administrative tasks on your target ESXi host. You can also use the VMware Host Client to conduct emergency management when vCenter Server is not available.

It is important to know that the VMware Host Client is different from the vSphere Web Client, regardless of their similar user interfaces. You use the vSphere Web Client to connect to vCenter Server and manage multiple ESXi hosts, whereas you use the VMware Host Client to manage a single ESXi host.

VMware Host Client functions include, but are not limited to the following operations:

- Basic virtualization operations, such as deploying and configuring virtual machines of various complexity
- Creating and managing networking and datastores
- Advanced tuning of host level options to improve performance

This chapter includes the following topics:

- [VMware Host Client System Requirements](#)
- [Using the VMware Host Client](#)

VMware Host Client System Requirements

Make sure that your browser supports the VMware Host Client.

The following guest operating systems and Web browser versions are supported for the VMware Host Client.

Supported Browsers	Mac OS	Windows	Linux
Google Chrome	50+	50+	50+
Mozilla Firefox	45+	45+	45+
Microsoft Internet Explorer	N/A	11+	N/A
Microsoft Edge	N/A	38+	N/A
Safari	9.0+	N/A	N/A

Using the VMware Host Client

The embedded VMware Host Client is an HTML5-based client that has a similar interface to the vSphere Web Client but is only used to manage single ESXi hosts. You use the VMware Host Client to conduct emergency management when vCenter Server is temporarily unavailable.

Start the VMware Host Client and Log In

You can use the VMware Host Client to manage single ESXi hosts and perform various administrative and troubleshooting tasks on your virtual machines.

Note The VMware Host Client only works for administrative users.

Procedure

- 1 In a Web browser enter the target host name or IP address using the form **http://host-name/ui** or **http://host-IP-address/ui**.

A log in screen appears.

- 2 Enter your user name and your password.
- 3 Click **Login** to continue.
- 4 Review the VMware Customer Experience Improvement Program (CEIP) page and choose whether you want to join the program.

To learn about the program and how to configure it at any time, see [Configuring Customer Experience Improvement Program](#).

- 5 Click **OK**.

You are now logged in to your target ESXi host.

Log Out of the VMware Host Client

When you no longer need to view or manage your target ESXi host, log out of the VMware Host Client.

Note Closing a VMware Host Client session does not stop the host.

Procedure

- ◆ To log out of the ESXi host, click the user name at the top of the VMware Host Client window and select **Log out** from the drop-down menu.

You are now logged out of the VMware Host Client. Your target ESXi host continues to run all its normal activities.

Configuring Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

Categories of Information That VMware Receives

This product participates in VMware's Customer Experience Improvement Program ("CEIP").

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>. To join or leave the CEIP for this product, see [Leave and Rejoin the Customer Experience Improvement Program in the VMware Host Client](#).

Leave and Rejoin the Customer Experience Improvement Program in the VMware Host Client

You can choose to leave the Customer Experience Improvement Program (CEIP), or rejoin the CEIP at any time.

Procedure

- 1 To leave and rejoin the CEIP, click the user name at the top of the VMware Host Client page.
- 2 Point to **Client settings**> **Send usage statistics**, to leave or rejoin the CEIP.

Host Management with the VMware Host Client

2

With the VMware Host Client, you can manage single ESXi hosts during vCenter Server upgrades or when vCenter Server stops responding or becomes unavailable.

The VMware Host Client has a crucial set of troubleshooting functions, which allow you to perform tasks on the ESXi host that you are logged in to if vCenter Server is unavailable. These functions include but are not limited to configuring advanced host settings, licensing, managing certificates, using the ESXi Shell, enabling Lockdown mode, and so on.

This chapter includes the following topics:

- [Managing System Settings in the VMware Host Client](#)
- [Managing Hosts in vCenter Server](#)
- [Reboot or Shut Down an ESXi Host in the VMware Host Client](#)
- [Using the ESXi Shell](#)
- [Place a Host in Maintenance Mode in the VMware Host Client](#)
- [Generate a Support Bundle in the VMware Host Client](#)
- [Monitoring an ESXi Host in the VMware Host Client](#)
- [Lockdown Mode](#)
- [Administering CPU Resources by Using the VMware Host Client](#)

Managing System Settings in the VMware Host Client

With the VMware Host Client, you can manage advanced host settings, assign or remove licenses to your host, configure start and stop policies for host services, and manage time and date configuration for the host.

Manage Advanced Settings in the VMware Host Client

You can change the settings of a host by using the VMware Host Client.

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 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
- 2 Right-click the appropriate item from the list and select **Edit option** from the drop-down menu.
The **Edit option** dialog box is displayed.
- 3 Edit the value and click **Save** to apply your changes.
- 4 (Optional) Right-click the appropriate item from the list and select **Reset to default** to go back to the original settings of the item.

Managing Hardware for an ESXi Host by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can manage PCI devices and configure power management settings.

Host Power Management Policies

You can apply several power management features in ESXi that the host hardware provides to adjust the balance between performance and power. You can control how ESXi uses these features by selecting a power management policy.

Selecting a high-performance policy provides more absolute performance, but at lower efficiency and performance per watt. Low-power policies provide less absolute performance, but at higher efficiency.

You can select a policy for the host that you manage by using the VMware Host Client. If you do not select a policy, ESXi uses Balanced by default.

Table 2-1. CPU Power Management Policies

Power Management Policy	Description
High Performance	Do not use any power management features.
Balanced (Default)	Reduce energy consumption with minimal performance compromise
Low Power	Reduce energy consumption at the risk of lower performance
Custom	User-defined power management policy. Advanced configuration becomes available.

When a CPU runs at lower frequency, it can also run at lower voltage, which saves power. This type of power management is typically called Dynamic Voltage and Frequency Scaling (DVFS). ESXi attempts to adjust CPU frequencies so that virtual machine performance is not affected.

When a CPU is idle, ESXi can apply deep halt states, also known as C-states. The deeper the C-state, the less power the CPU uses, but it also takes longer for the CPU to start running again. When a CPU becomes idle, ESXi applies an algorithm to predict the idle state duration and chooses an appropriate C-state to enter. In power management policies that do not use deep C-states, ESXi uses only the shallowest halt state for idle CPUs, C1.

Change Power Management Policies in the VMware Host Client

Change the power management policies of the host that you are managing to control the energy consumption of your host.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Hardware**.
- 2 Click **Power Management** and click **Change policy**.
The available power management policies are displayed.
- 3 Select the radio button next to the policy that you want to apply.
- 4 Click **OK**.

Licensing for ESXi Hosts

ESXi hosts are licensed with vSphere licenses. Each vSphere license has a certain CPU capacity that you can use to license multiple physical CPUs on ESXi hosts. When you assign a vSphere license to a host, the amount of CPU capacity that is consumed is equal to the number of physical CPUs in the host. vSphere Desktop that is intended for VDI environments is licensed on per virtual machine basis.

To license an ESXi host, you must assign it a vSphere license that meets the following prerequisites:

- The license must have sufficient CPU capacity to license all physical CPUs on the host. For example, to license two ESXi hosts that have four CPUs each, you need to assign a vSphere license with a minimum capacity of 8 CPUs to the hosts.
- The license must support all the features that the host uses. For example, if the host is associated with a vSphere Distributed Switch, the license that you assign must support the vSphere Distributed Switch feature.

If you attempt to assign a license that has insufficient capacity or does not support the features that the host uses, the license assignment fails.

You can assign and reassign the CPU capacity of a vSphere license to any combination of ESXi hosts. . You can assign a vSphere license for 10 CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts
- Three 2-CPU hosts and one 4-CPU host
- Two 4-CPU hosts and one 2-CPU host
- One 8-CPU host and one 2-CPU host

Dual-core and quad-core CPUs, such as Intel CPUs that combine two or four independent CPUs on a single chip, count as one CPU.

Evaluation Mode

When you install ESXi, its default license is evaluation mode. Evaluation mode licenses expire after 60 days. An evaluation mode license provides the set of features that equals the highest vSphere product edition.

If you assign a license to an ESXi host before its evaluation period expires, the time available in the evaluation period is decreased by the time already used. To explore the entire set of features that are available for the host, you can set it back to evaluation mode, and use it for the remaining evaluation period.

For example, if you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard license to the host and then set the host back to evaluation mode, you can explore the entire set of features that are available for the host for the remaining evaluation period of 40 days.

License and Evaluation Period Expiry

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused while the host was in evaluation mode.

Licensing ESXi Hosts After Upgrade

If you upgrade an ESXi host to a version that starts with the same number, you do not need to replace the existing license with a new one. For example, if you upgrade a host from ESXi 5.1 to 5.5, you can use the same license for the host.

If you upgrade an ESXi host to a version that starts with a different number, you must apply a new license. For example, if you upgrade an ESXi host from 5.x to 6.x, you need to license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license usage for vSphere Desktop equals the total number of powered on desktop virtual machines running on the hosts that are assigned a vSphere Desktop license.

View Licensing Information About the VMware Host Client Environment

You can view the available licenses in the VMware Host Client along with their expiration dates, license key, and various features. You can also view the available products and assets.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Licensing**.
- 2 Click a license from the list to view the license key, expiration date, and the available features and assets.

Assign a License Key to an ESXi Host in the VMware Host Client

By using the VMware Host Client, you can assign an existing or new license key to an ESXi host.

Prerequisites

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

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Licensing**.
- 2 Click **Assign license**, enter a license key in the form `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`, and click **Check license**.
- 3 Click **Assign license** to save your changes.

Remove a License from an ESXi Host in the VMware Host Client

To remain in compliance with the licensing models of products that you use with vSphere, you must remove all unassigned licenses from the inventory. If you have divided, combined, or upgraded licenses in My VMware, you must remove the old licenses.

For example, suppose that you have upgraded a vSphere license from 5.5 to 6.0 in My VMware. You assign the license to ESXi 6.0 hosts. After assigning the new vSphere 6.0 licenses, you must remove the old vSphere 5.5 license from the inventory.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Licensing**.
- 2 Right-click a license from the list, click **Remove license**, and click **Remove**.

Update Your VMware Host Client Environment to the Latest Version

To evaluate whether you are using the latest version of the VMware Host Client, check what VIBs are installed to your environment and examine the VIBs version information. You can update your VMware Host Client environment by entering a URL to a VIB or an ESX update `metadata.zip` file.

If you provide a VIB, an existing VIB that is installed to your VMware Host Client environment is updated to the new VIB.

If a link to a `metadata.zip` file is provided, the entire ESXi system is updated to the version described by the `metadata.zip` file.

Caution If the host is managed by vSphere Update Manager, updating the host via this message might cause Update Manager to report the host as non-compliant.

Procedure

- 1 Click **Manage** in the VMware Host Client and click **Packages**.

- 2 Click **Install update** and enter the URL of the VIB or a `metadata.zip` file.
- 3 Click **Update**.
- 4 Click **Refresh** to make sure that the update is successful.

Manage Services in the VMware Host Client

In the VMware Host Client, you can start, stop, and restart services that are running on the host that you are logged in to, and you can configure host service policy. You can restart services when you change host configurations or in case of suspected functional or performance issues.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Services**.
- 2 From the **Services** list, select a service.
- 3 From the **Actions** drop-down menu, select an operation.
 - **Restart**
 - **Start**
 - **Stop**
- 4 (Optional) From the **Actions** drop-down menu, select **Policy** and select an option for the service from the menu.
 - **Start and stop with firewall ports**
 - **Start and stop with host**
 - **Start and stop manually**

Managing Security and Users for an ESXi Host by Using the VMware Host Client

The ESXi hypervisor architecture has many built-in security features that you can configure to enhance security. By using the VMware Host Client, you can configure features, such as active directory, and you can also manage certificates.

Managing Host Authentication by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can check whether active directory and smart card authentication are enabled, and you can also join the host to a directory service domain.

Join an ESXi Host to a Directory Service Domain by Using the VMware Host Client

To use a directory service for your host, 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, see *vSphere Security*.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
- 2 Click **Authentication** and click **Join domain**.
- 3 Enter a domain name.
Use the form **name.tld** or **name.tld/container/path**.
- 4 Enter the user name and password of a directory service user account that has permissions to join the host to the domain and click **Join domain**.
- 5 (Optional) If you intend to use an authentication proxy, enter the proxy server IP address and click **Join domain**.

Using Active Directory to Manage ESXi 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.

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.

vSphere Authentication Proxy is especially useful when used with Auto Deploy. You can set up a reference host that points to Authentication Proxy and set up a rule that applies the reference host's profile to any ESXi host provisioned with Auto Deploy. Even if you use vSphere Authentication Proxy in an environment that uses certificates that are provisioned by VMCA or third-party certificates, the process works seamlessly as long as you follow the instructions for using custom certificates with Auto Deploy. See the *vSphere Security* guide.

Note You cannot use vSphere Authentication Proxy in an environment that supports only IPv6.

Managing Host Certificates by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can view the certificate details of your host, such as the issuer and the validity period, and you can also import new certificates

View Certificate Details for an ESXi Host in the VMware Host Client

For ESXi 6.0 and later, hosts that are in VMCA mode or custom mode, you can view certificate details when you are logged in to the host with the VMware Host Client. The certificate information can be useful for debugging.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
- 2 Click **Certificates**.

You can view the following certificate details.

Field	Description
Issuer	The issuer of the certificate.
Not valid after	Date on which the certificate expires.
Not valid before	Date on which the certificate is generated.
Subject	The subject used during certificate generation.

Import a New Certificate for an ESXi Host in the VMware Host Client

You can import a certificate from a trusted certificate authority when you are logged in to an ESXi host with the VMware Host Client.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
- 2 Click **Certificates** and click **Import new certificate**.
- 3 Generate a certificate signing request, which is either an FQDN signing request or an IP signing request.

The certificate signing request is then passed to the certificate authority to generate the official certificate.

An FQDN request has the fully qualified hostname of the host in the resulting common name field of the certificate. The IP signing request has the current IP address of the host in the common name field.

- 4 Paste a PEM formatted certificate in the certificate text box and click **Import**.

You do not have to import the certificate immediately but you cannot reboot the host between generating the certificate signing request and importing the certificate.

Edit Time Configuration of an ESXi Host in the VMware Host Client

You can configure the time settings on a host manually, or you can synchronize the time and date of the host by using an NTP server.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Time & Date**.

- 2 Click **Edit settings**.
- 3 Select an option for setting the time and date of the host.

Option	Description
Manually configure the date and time on this host	Set the time and date for the host manually.
Use Network Time Protocol (Enable NTP client)	<p>Synchronize the time and date of the host with an NTP server. The NTP service on the host periodically takes the time and date from the NTP server.</p> <ol style="list-style-type: none"> a In the NTP Servers text box, type the IP addresses or host names of the NTP servers that you want to use. b From the NTP Service Startup Policy drop-down list, select an option for starting and stopping the NTP service on the host. <ul style="list-style-type: none"> ■ Start and stop with port usage - Starts or stops the NTP service when the NTP client port is enabled or disabled for access in the security profile of the host . ■ Start and stop with host - Starts and stops the NTP service when the host powers on or shuts down. ■ Start and stop manually - Enables manual starting and stopping of the NTP service. <p>You can use the Start, Stop, or Restart buttons to control the status of the NTP service on the host manually at any time regardless of the selected startup policy for the NTP service. If you select the Start and stop manually policy, the status of the NTP service only changes when you use the UI controls. .</p>

- 4 Click **Save settings**.

Managing Hosts in vCenter Server

To access the full capabilities of the host that you are managing, connect the host to a vCenter Server system.

For information about configuration management of ESXi hosts, see the *vSphere Networking* documentation, the *vSphere Storage* documentation, and the *vSphere Security* documentation.

Switch to the vSphere Web Client

To access the full set of capabilities, and advanced administrative and troubleshooting functions of the ESXi host, connect the ESXi host to vCenter Server.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Manage with vCenter Server** from the drop-down menu.

The vCenter Server login page opens in a new window.
- 2 Enter your credentials and click **Login**.

Disconnect an ESXi Host from vCenter Server by Using the VMware Host Client

If you no longer want to use the advanced set of capabilities available through vCenter Server for host management, or if vCenter Server has failed and you must perform emergency operations on the host, you can disconnect your ESXi host from vCenter Server.

Disconnecting an ESXi host might take up to several minutes.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Disconnect from vCenter Server** from the pop-up menu.

Note Disconnecting a host signals vCenter Server that this host is not responding.

- 2 Click **Disconnect from vCenter Server**.

Reboot or Shut Down an ESXi Host in the VMware Host Client

You can power off or restart any ESXi host by using the VMware Host Client. Powering off a managed host disconnects it from vCenter Server, but does not remove it from the inventory.

Prerequisites

To be able to reboot or shut down a host, you need these privileges.

- **Host.Configuration.Maintenance**
- **Global.Log event**

Always perform the following tasks before you reboot or shut down a host:

- Power off all virtual machines on the host.
- Place the host in maintenance mode.

Procedure

- 1 Right-click the host, select **Shut down host** or **Reboot host**.

Note If the host is not in maintenance mode, shutting down or rebooting it does not stop the virtual machines that are running on this host safely and unsaved data may be lost. If the host is part of a Virtual SAN cluster, you might lose access to the Virtual SAN data on the host.

- 2 Click **Shut down** or **Reboot** to complete the procedure.

Using the ESXi Shell

The ESXi Shell, which was formerly referred to as Tech Support Mode or TSM, is disabled by default on ESXi. You can enable local and remote access to the shell if necessary.

Enable the ESXi Shell for troubleshooting only. The ESXi Shell can be enabled or disabled when the host is running in lockdown mode. The host running in lockdown mode does not prevent you from enabling or disabling the ESXi Shell. See *vSphere Security*.

ESXi Shell	Enable this service to access the ESXi Shell locally.
SSH	Enable this service to access the ESXi Shell remotely by using SSH. See <i>vSphere Security</i> .

The root user and users with the Administrator role can access the ESXi Shell. Users who are in the Active Directory group ESX Admins are automatically assigned the Administrator role. By default, only the root user can execute system commands (such as `vmware -v`) by using the ESXi Shell.

Note Do not enable the ESXi Shell until you actually need access.

Enable the Secure Shell (SSH) in the VMware Host Client

Enable the Secure Shell (SSH) to access the ESXi Shell remotely by using SSH.

Procedure

- 1 To enable or disable the Secure Shell (SSH), right-click **Host** in the VMware Host Client inventory.
- 2 Select **Services** from the drop-down menu and select **Secure Shell (SSH)**.
- 3 Select a task to perform.
 - If SSH is enabled, click **Disable** to disable it.
 - If SSH is disabled, click **Enable** to enable it.

Enable the ESXi Console Shell in the VMware Host Client

When you enable this service while running in lockdown mode, you can log in locally to the direct console user interface as the root user and disable lockdown mode. You can then access the host using a direct connection to the VMware Host Client or by enabling the ESXi Shell.

Procedure

- 1 To enable or disable the Console Shell, right-click **Host** in the VMware Host Client inventory.
- 2 Select **Services** from the drop-down menu and select **Console Shell**.
- 3 Select a task to perform.
 - If the Console Shell is enabled, click **Disable** to disable it.
 - If the Console Shell is disabled, click **Enable** to enable it.

Place a Host in Maintenance Mode in the VMware Host Client

You place a host in maintenance mode when you need to service it, for example, to install more memory. A host enters or leaves maintenance mode only as the result of a user request.

The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered off or migrated to different hosts. You cannot power off virtual machines or migrate virtual machines to a host that is entering or in maintenance mode.

To place a host in maintenance mode, all virtual machines that are running on the host must be powered off or migrated to different hosts. If you attempt to place a host that has running virtual machines on it in maintenance mode, DRS must power off or migrate the running virtual machines for the task to complete. If a time out occurs before the virtual machines are powered off or migrated, an error message appears.

When all virtual machines on the host are inactive, the host's icon displays **under maintenance** and the host's Summary panel indicates the new state. While in maintenance mode, the host does not allow you to deploy or power on a virtual machine.

Prerequisites

Before you place a host in maintenance mode, power off all virtual machines that are running on that host or migrate them to another host either manually or automatically by DRS.

Procedure

- ◆ Right-click the host and select **Enter maintenance mode**.

The host is in maintenance mode until you select **Exit maintenance mode**.

Generate a Support Bundle in the VMware Host Client

You can generate a support bundle for the ESXi host that you are logged in on. The support bundle contains the log files and system information that you can use to diagnose and resolve problems.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Generate support bundle** from the drop-down menu.

A dialog that contains a link to download the bundle pops up when the support bundle is created.

- 2 (Optional) Click **Monitor** in the VMware Host Client inventory, click **Tasks** and click a log bundle from the list.

You can view the link to the log bundle under the table.

Monitoring an ESXi Host in the VMware Host Client

When you connect to a host using the VMware Host Client, you can monitor the host health status, and view performance charts, events, tasks, system logs, and notifications.

View Charts in the VMware Host Client

When you are logged in to the VMware Host Client, you can view information about resource usage of the ESXi host that you are managing in line chart form.

To reduce memory consumption, the VMware Host Client only contains statistics for the last hour.

Procedure

- 1 Click **Monitor** in the VMware Host Client and click **Performance**.
- 2 (Optional) To view the host usage for the last hour, select an option from the drop-down menu.
 - To view the percentage of CPU that the host used during the last hour, select **CPU**.
 - To view the percentage of memory that the host consumed during the last hour, select **Memory**.
 - ◆ To view the memory and CPU composite that the host consumed during the last hour, select **CPU + memory composite**.
 - ◆ To view the percentage of network that the host consumed during the last hour, select **Network**.
 - ◆ To view the disk usage that the host consumed during the last hour, select **Disk**.

Monitor Hardware Health Status in the VMware Host Client

When you are logged in to the VMware Host Client, you can monitor the health status of the ESXi host hardware.

Note Hardware health status is only available when the underlying hardware supports it.

Procedure

- 1 Click **Monitor** in the VMware Host Client inventory and click **Hardware**.
- 2 Select the type of information to view.
- 3 (Optional) Use the filter controls above the list to filter the list.
- 4 (Optional) Click a column heading to sort the list.

View Events in the VMware Host Client

Events are records of user actions or system actions that occur on an ESXi host. When you are logged in to the VMware Host Client, you can view all events associated with the host that you are managing.

Prerequisites

Required privilege: **Read-only**.

Procedure

- ◆ Click **Monitor** in the VMware Host Client inventory and click **Events**.
 - a (Optional) Select an event to see event details.
 - b (Optional) Use the filter controls above the list to filter the list.
 - c (Optional) Click a column heading to sort the list.

View Tasks in the VMware Host Client

When you are logged in to the VMware Host Client, you can view tasks that are related to the ESXi host. You can view information about task initiator, task state, task result, task description, and so on.

Procedure

- ◆ Click **Monitor** in the VMware Host Client inventory and click **Tasks**.
 - a (Optional) Select a task to see task details.
 - b (Optional) Use the filter controls above the list to filter the list.
 - c (Optional) Click a column heading to sort the list.

View System Logs in the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can view log entries to get information such as who generated an event, when the event was created, and the type of event.

Procedure

- 1 Click **Monitor** in the VMware Host Client inventory and click **Logs**.

The list of logs is displayed.
- 2 (Optional) Click on a log to view log details.
- 3 (Optional) Right-click a log and select one of the following options:
 - **Open in new window**
 - **Generate support bundle**

View Notifications in the VMware Host Client

When you are logged in the VMware Host Client, you can view host notifications and recommendations for related tasks that you should perform.

Procedure

- 1 Click **Monitor** in the VMware Host Client inventory and click **Notifications**.
- 2 Select a notification from the list to view the recommended action.

A message with a recommended action and a description is displayed under the notifications list.

Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode. In lockdown mode, operations must be performed through vCenter Server by default.

Normal Lockdown Mode and Strict Lockdown Mode

With vSphere 6.0, you can select normal lockdown mode or strict lockdown mode.

Normal Lockdown Mode

In normal lockdown mode, the DCUI service remains active. If the connection to the vCenter Server system is lost, and access through the vSphere Web Client is unavailable, privileged accounts can log in to the ESXi host's Direct Console Interface and exit lockdown mode. Only the following accounts can access the Direct Console User Interface:

- Accounts in the Exception User list for lockdown mode who have administrative privileges on the host. The Exception Users list is meant for service accounts that perform specific tasks. Adding ESXi administrators to this list defeats the purpose of lockdown mode.
- Users defined in the DCUI.Access advanced option for the host. This option is for emergency access to the Direct Console Interface in case the connection to vCenter Server is lost. These users do not require administrative privileges on the host.

Strict Lockdown Mode

In strict lockdown mode, which is new in vSphere 6.0, the DCUI service is stopped. If the connection to vCenter Server is lost and the vSphere Web Client is no longer available, the ESXi host becomes unavailable, unless the ESXi Shell and SSH services are enabled and Exception Users are defined. If you cannot restore the connection to the vCenter Server system, you must reinstall the host.

Lockdown Mode and the ESXi Shell and SSH Services

Strict lockdown mode stops the DCUI service. However, the ESXi Shell and SSH services are independent of lockdown mode. For lockdown mode to be an effective security measure, ensure that ESXi Shell and SSH services are also disabled. These services are disabled by default.

When a host is in lockdown mode, users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option.

Note The Exception Users list is meant for service accounts that perform specific tasks such as host backups, and not for administrators. Adding administrator users to the Exception Users list defeats the purpose of lockdown mode.

Put an ESXi Host in Normal Lockdown Mode by Using the VMware Host Client

You can use the VMware Host Client to enter normal lockdown mode.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Enter normal lockdown**.

A warning message appears.

- 2 Click **Enter normal lockdown**.

Put an ESXi Host in Strict Lockdown Mode by Using the VMware Host Client

You can use the VMware Host Client to enter strict lockdown mode.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Enter strict lockdown**.

The warning message appears.

- 2 Click **Enter strict lockdown**.

Exit Lockdown Mode by Using the VMware Host Client

If you have entered normal or strict lockdown mode on an ESXi host, you can exit lockdown by using the VMware Host Client.

Procedure

- ◆ Right-click **Host** in the VMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Exit lockdown**.

Specify Lockdown Mode Exception Users in the VMware Host Client

Starting with vSphere 6.0, you can add users to the exception users list by using the VMware Host Client. These users do not lose their permissions when the host enters lockdown mode. You can add service accounts, such as a backup agent to the exception users list.

Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. They are not members of an Active Directory group and are not vCenter Server users. These users are allowed to perform operations on the host based on their privileges. That means, for example, that a read-only user cannot disable lockdown mode on a host.

Note The exception users list is useful for service accounts that perform specific tasks, such as host backups, and not for administrators. Adding administrator users to the exception users list defeats the purpose of lockdown mode.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
- 2 Click **Lockdown mode**.
- 3 Click **Add user exception**, enter the name of the user, and click **Add exception**.
- 4 (Optional) Select a name from the exception users list, click **Remove user exception**, and click **Confirm**.

Administering CPU Resources by Using the VMware Host Client

When you connect to an ESXi host with the VMware Host Client, you have access to a limited number of resource management settings.

View Processor Information by Using the VMware Host Client

In the VMware Host Client, you can access information about the current CPU configuration of the ESXi host that you are logged in to.

Procedure

- 1 Click **Host** in the VMware Host Client inventory.
- 2 Expand **Hardware** and expand **CPU**.

You can view the information about the number and type of physical processors, and the number of logical processors.

Assign a Virtual Machine to a Specific Processor in the VMware Host Client

By using CPU affinity, you can assign a virtual machine to a specific processor. This way, you can assign a virtual machine only to a particular available processor in multiprocessor systems.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Right-click the virtual machine in the VMware Host Client inventory and select **Edit settings**.
- 2 Under **Virtual Hardware**, expand **CPU**.
- 3 Under **Scheduling Affinity**, select physical processor affinity for the virtual machine.
Use a hyphen to indicate ranges and a comma to separate values.
For example, **0, 2, 4-7** would indicate processors 0, 2, 4, 5, 6, and 7.
- 4 Click **Save** to apply your changes.

Virtual Machine Management with the VMware Host Client

3

Virtual machines can be configured like physical computers and can perform the same tasks as physical computers. Virtual machines also support special features that physical computers do not support.

You can use the VMware Host Client to create, register, and manage virtual machines, and to conduct daily administrative and troubleshooting tasks.

This chapter includes the following topics:

- [Creating a Virtual Machine in the VMware Host Client](#)
- [Deploying a Virtual Machine from an OVF or OVA File in the VMware Host Client](#)
- [Registering an Existing Virtual Machine in the VMware Host Client](#)
- [Using Consoles in the VMware Host Client](#)
- [Managing a Guest Operating System in the VMware Host Client](#)
- [Configuring a Virtual Machine in the VMware Host Client](#)
- [Managing Virtual Machines in the VMware Host Client](#)
- [Monitoring a Virtual Machine in the VMware Host Client](#)

Creating a Virtual Machine in the VMware Host Client

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 with a particular datastore and select an operating system and virtual hardware options. After you power on the virtual machine, it consumes resources dynamically as the workload increases, or 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.

1 [Start the Virtual Machine Creation Process in the VMware Host Client](#)

You use the **New Virtual Machine** wizard to create a virtual machine to place in the VMware Host Client inventory.

2 [Select a Method for Adding a New Virtual Machine on the Host with the VMware Host Client](#)

You use the Select creation type page of the **New Virtual Machine** wizard to create a new virtual machine, deploy a virtual machine from an OVF or OVA file, or register an existing virtual machine.

3 [Select a Name and a Guest Operating System for the Virtual Machine in the VMware Host Client](#)

When you create a new virtual machine, provide a unique name for the virtual machine to distinguish it from existing virtual machines on the host you are managing. After you select a guest operating system, the wizard provides the appropriate defaults for the operating system installation.

4 [Select a Storage for Your Virtual Machine in the VMware Host Client](#)

Select the datastore or datastore cluster to store the virtual machine configuration files and all of the virtual disks in. You can select the datastore that has the most suitable properties, such as size, speed, and availability, for your virtual machine storage.

5 [Customize the Virtual Machine Settings in the VMware Host Client](#)

Before you deploy a new virtual machine, you have the option to configure the virtual machine hardware and the virtual machine options.

6 [Complete Virtual Machine Creation in the VMware Host Client](#)

In the Ready to complete page, you review the configuration selections that you made for the virtual machine.

Start the Virtual Machine Creation Process in the VMware Host Client

You use the **New Virtual Machine** wizard to create a virtual machine to place in the VMware Host Client inventory.

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 close the wizard without completing all tasks, you cannot resume the wizard where you left off. You must start a new creation task.

Prerequisites

Verify that you have the **VirtualMachine.Inventory.Create** privileges.

Depending on the properties of the virtual machine you want to create, you might need the following additional privileges:

- **VirtualMachine.Config.AddExistingDisk** if including a virtual disk device that refers to an existing virtual disk file (not RDM).
- **VirtualMachine.Config.AddNewDisk** if including a virtual disk device that creates a new virtual disk file (not RDM).
- **VirtualMachine.Config.RawDevice** if including a raw device mapping (RDM) or SCSI passthrough device.
- **VirtualMachine.Config.HostUSBDevice** if including a VirtualUSB device backed by a host USB device.
- **VirtualMachine.Config.AdvancedConfig** if setting values in `ConfigSpec.extraConfig`.
- **VirtualMachine.Config.SwapPlacement** if setting `swapPlacement`.

- **VirtualMachine.Config.ChangeTracking** if setting changed block tracking for the virtual machine disks.
- **Datastore.AllocateSpace** required on all datastores where the virtual machine and its virtual disks are created.
- **Network.Assign** required on the network which is assigned to the new virtual machine that is being created.

Procedure

- ◆ Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.

The **New Virtual Machine** wizard opens.

Select a Method for Adding a New Virtual Machine on the Host with the VMware Host Client

You use the Select creation type page of the **New Virtual Machine** wizard to create a new virtual machine, deploy a virtual machine from an OVF or OVA file, or register an existing virtual machine.

Procedure

- ◆ Select a creation type and click **Next**.

Option	Description
Create a new virtual machine	Creates a new virtual machine. You can customize processors, memory, network connections, and storage. You will need to install a guest operating system after you create the VM.
Deploy a virtual machine from an OVF or OVA file	Deploys a virtual machine from an OVF and VMDK files. OVA deployment is currently limited to files under 1 gigabyte in size due to Web browser limitations. If you want to deploy an OVA greater than 1 gigabyte, extract the OVA using tar and provide the OVF and VMDK files separately.
Register an existing virtual machine	Registers a virtual machine that already exists on a datastore.

Select a Name and a Guest Operating System for the Virtual Machine in the VMware Host Client

When you create a new virtual machine, provide a unique name for the virtual machine to distinguish it from existing virtual machines on the host you are managing. After you select a guest operating system, the wizard provides the appropriate defaults for the operating system installation.

The following procedure applies if you want to create a new virtual machine.

Procedure

- 1 Enter a name for your virtual machine.
- 2 Select the virtual machine compatibility from the **Compatibility** drop-down menu.
- 3 Select the guest operating system family from the **Guest OS family** drop-down menu.

- 4 Select a guest operating system version from the **Guest OS version** drop-down menu.
- 5 Click **Next**.

Select a Storage for Your Virtual Machine in the VMware Host Client

Select the datastore or datastore cluster to store the virtual machine configuration files and all of the virtual disks in. You can select the datastore that has the most suitable properties, such as size, speed, and availability, for your virtual machine storage.

Procedure

- 1 In the list of accessible datastores, on the Select storage page of the **New Virtual Machine** wizard, click the destination datastore that you want to store the virtual machine configuration files and all of the virtual disks in.
- 2 Click **Next**.

Customize the Virtual Machine Settings in the VMware Host Client

Before you deploy a new virtual machine, you have the option to configure the virtual machine hardware and the virtual machine options.

For information about virtual machine options and virtual disk configuration, including instructions for adding different types of devices, see *vSphere Virtual Machine Administration*.

Procedure

- 1 Configure the virtual machine hardware settings on the **Virtual Hardware** tab of the Customize settings page in the **New Virtual Machine** wizard.
- 2 (Optional) To add a new virtual hardware device, select the device from the **Add other device** drop-down menu on the Customize settings page of the **New Virtual Machine** wizard.
- 3 (Optional) Expand any device to view and configure device settings.

Option	Description
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. The number of virtual CPUs that are available to a virtual machine depends on the number of licensed CPUs on the host, and the number of CPUs supported by the guest operating system. To use the VMware multicore virtual CPUs feature, you must comply with the requirements of the guest operating system EULA.
Memory	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. 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.

Option	Description
Hard disk	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.
SCSI controller	Storage controllers appear to a virtual machine as different types of SCSI controllers, including BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual SCSI. 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.
SATA controller	If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you spread the devices among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the thirty-device limit for a single controller. You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.
Network adapter	When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type. The type of network adapters that are available depend on the following factors: <ul style="list-style-type: none"> ■ The virtual machine compatibility, which depends on the host that created or most recently updated it. ■ Whether the virtual machine compatibility has been updated to the latest version for the current host. ■ The guest operating system.
CD/DVD drive	You can configure DVD or CD devices to connect to client devices, host devices, or Datastore ISO files.

- 4 To remove a device, click the delete button  next to the device.

This option appears only for virtual hardware that you can remove safely.

- 5 Configure the virtual machine options on the **VM Options** tab of the Customize settings page in the **New Virtual Machine** wizard.
- 6 Click **Next**.

Complete Virtual Machine Creation in the VMware Host Client

In the Ready to complete page, you review the configuration selections that you made for the virtual machine.

Procedure

- 1 On the Ready to complete page of the **New Virtual Machine** wizard, review the configuration settings for the virtual machine.
- 2 (Optional) Click **Back** to go back and review the wizard settings.
- 3 (Optional) Click **Cancel** to discard the creation task and close the wizard.
- 4 Click **Finish** to complete the creation task and close the wizard.

The virtual machine appears in the VMware Host Client inventory under **Virtual Machines**.

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.

You can map the virtual machine's CDROM/DVD to an ISO file and start the virtual machine. This triggers the operating system install.

Deploying a Virtual Machine from an OVF or OVA File in the VMware Host Client

When you connect to an ESXi host by using the VMware Host Client, you can deploy virtual machines from OVF and VMDK files, and from OVA files.

1 [OVF and OVA Limitations for the VMware Host Client](#)

You can create a virtual machine in the VMware Host Client by using OVF and VMDK files, or OVA files. However, several limitations are applicable to this deployment method .

2 [Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client](#)

Use the **New Virtual Machine** wizard to deploy virtual machines from OVF and VMDK files, or from OVA files.

3 [Select OVF and VMDK, or OVA Files to Deploy in the VMware Host Client](#)

Select the OVF and VMDK files, or OVA file for the virtual machine that you would like to deploy.

4 [Select Storage in the VMware Host Client](#)

Select the datastore in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties.

5 [Complete the Deployment of a Virtual Machine from an OVF or OVA File in the VMware Host Client](#)

In the Ready to complete page, review the configuration selections that you made for the virtual machine.

OVF and OVA Limitations for the VMware Host Client

You can create a virtual machine in the VMware Host Client by using OVF and VMDK files, or OVA files. However, several limitations are applicable to this deployment method .

OVA Limitations

You can upload OVA files by using either a Web browser or a client. The memory requirements are significant and might cause the Web browser to stop responding or make the system unstable. The size of the OVA file that can be uploaded depends on how much memory is available on your system. VMware tests show that Google Chrome can upload OVA files of about 1 gigabyte. Mozilla Firefox can extract larger OVA files, but might become unresponsive.

To deploy a large OVA file, VMware recommends to first extract the OVA on your system by running the command `tar -xvf <file.ova>`. Then you can provide the deployment wizard with the OVF and VMDKs as separate files.

OVF Limitations

The size of OVF files that a Web browser can upload are also limited. Different Web browsers have different file size limits. Recent versions of Internet Explorer can upload OVF files up to 4 gigabytes in size. Mozilla Firefox also has a 4 gigabyte limit. Google Chrome can handle larger files and there is no documented limit.

Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client

Use the **New Virtual Machine** wizard to deploy virtual machines from OVF and VMDK files, or from OVA files.

OVA deployment is limited to files under 1 gigabyte in size due to Web browser limitations. If you want to deploy an OVA file greater than 1 gigabyte, extract the OVA file using tar and provide the OVF and VMDK files separately.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM** .
The **New Virtual Machine** wizard opens.
- 2 On the Select creation type page of the wizard, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

Select OVF and VMDK, or OVA Files to Deploy in the VMware Host Client

Select the OVF and VMDK files, or OVA file for the virtual machine that you would like to deploy.

Procedure

- 1 Enter a name for your virtual machine.
Virtual machine names can contain up to 80 characters and must be unique within each ESXi instance.
- 2 Click the blue pane to select an OVF and a VMDK, or an OVA file to deploy.
Your local system storage opens.
- 3 Select the file that you want to deploy your virtual machine from and click **Open**.
The file you selected is displayed in the blue pane.
- 4 Click **Next**.

Select Storage in the VMware Host Client

Select the datastore in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties.

Procedure

- 1 Click a datastore from the list of accessible datastores on the Select storage page of the **New Virtual Machine** wizard.
- 2 Click **Next**.

Complete the Deployment of a Virtual Machine from an OVF or OVA File in the VMware Host Client

In the Ready to complete page, review the configuration selections that you made for the virtual machine.

Procedure

- 1 On the Ready to complete page of the **New Virtual Machine** wizard, review the configuration settings for the virtual machine.
- 2 (Optional) Click **Back** to go back and review the wizard settings.
- 3 (Optional) Click **Cancel** to discard the creation task and close the wizard.
- 4 Click **Finish** to complete the creation task and close the wizard.

The virtual machine appears in the VMware Host Client inventory under **Virtual Machines**.

Registering an Existing Virtual Machine in the VMware Host Client

With the VMware Host Client, you can register a single virtual machine or multiple virtual machines that already exist on a datastore in the host that you are managing.

1 [Register an Existing Virtual Machine in the VMware Host Client](#)

If you remove a virtual machine from the inventory of the host that you are managing but not from the host datastore, you can return the virtual machine to the host inventory by registering the virtual machine with the VMware Host Client.

2 [Select a Virtual Machine to Register in the VMware Host Client](#)

If you remove a virtual machine from a datastore but you do not delete the virtual machine from the host that you are managing, you can register the virtual machine on the datastore.

3 [Complete Virtual Machine Registration in the VMware Host Client](#)

Review your selections for virtual machine registration and complete the registration.

Register an Existing Virtual Machine in the VMware Host Client

If you remove a virtual machine from the inventory of the host that you are managing but not from the host datastore, you can return the virtual machine to the host inventory by registering the virtual machine with the VMware Host Client.

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.
The **New Virtual Machine** wizard opens.
- 2 Select **Register an existing virtual machine** and click **Next**.

Select a Virtual Machine to Register in the VMware Host Client

If you remove a virtual machine from a datastore but you do not delete the virtual machine from the host that you are managing, you can register the virtual machine on the datastore.

Procedure

- 1 In the Datastore browser dialog box, browse to and select the virtual machine configuration file, *filename.vmx*, and click **Select**.
- 2 (Optional) On the Select VMs for registration page, select another virtual machine to register if you want to register more than one virtual machine simultaneously.
- 3 Click **Next**.

Complete Virtual Machine Registration in the VMware Host Client

Review your selections for virtual machine registration and complete the registration.

Procedure

- ◆ Review your selections in the Ready to complete page of the **New Virtual Machine** wizard and click **Finish** to register your virtual machine.

Using Consoles in the VMware Host Client

You can access a virtual machine through a browser console or through VMware Remote Console (VMRC) in the VMware Host Client and perform different tasks on the virtual machine.

Using Browser Console

Note The browser console is not supported for any version of ESXi prior to 6.0. You must use VMRC in order to access the browser console.

You can use a browser console to gain access to the guest operating system without installing additional software. For additional console functionalities, such as attaching local hardware, install VMware Remote Console.

Note Currently browser consoles support only US, Japanese and German keyboard layouts. You must select the desired keyboard layout before opening the console.

Using VMware Remote Console

For a full set of console features, you can download and install VMRC. You can perform a variety of tasks on the virtual machine, such as restarting and shutting down the virtual machine guest operating system, resuming and suspending the virtual machine, configuring VMware Tools updates, configuring and managing the virtual machine and different devices, and so on. VMware Workstation™, VMware Fusion™ or VMware Player™ work as VMRC clients so you do not need to download and install VMRC if you have any of the three installed on your system.

Open a Virtual Machine Console in the VMware Host Client

With the VMware Host Client, you can access the desktop of a virtual machine by launching a console to the virtual machine. From the console, you can perform tasks in the virtual machine, such as configuring operating system settings, running applications, monitoring performance, and so on.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Select a powered-on virtual machine from the list.
- 3 Click **Console** and select an option from the drop-down menu.
 - Select **Open browser console** to view the virtual machine console in a pop-up window.
 - Select **Open console in new window** to view the virtual machine console in a separate window.

About VMware Remote Console

VMware Remote Console, also referred to as VMRC, provides access to virtual machines on remote hosts and performs console and device operations, such as configuring operating system settings and monitoring the virtual machine console for *VMware vSphere*. VMware Remote Console can also modify virtual machine settings such as RAM, CPU cores, and disks.

For a complete set of console features, download VMware Remote Console.

Install the VMware Remote Console Application in the VMware Host Client

The VMware Remote Console (VMRC) is a stand-alone console application for Windows that enables you to connect to client devices and launch virtual machine consoles on remote hosts.

Procedure

- 1 Click on **Virtual Machines** in the VMware Host Client inventory.
The list of virtual machines available on the host is displayed.
- 2 Select a virtual machine from the list.
- 3 Click **Actions**, select **Console** from the drop-down menu, and click **Download VMRC**.

Launch Remote Console for a Virtual Machine in the VMware Host Client

You can access virtual machines in the VMware Host Client by using VMware Remote Console. You can launch one or more consoles to access several remote virtual machines at the same time.

Prerequisites

Verify that VMware Remote Console is installed on your local system.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory and select a virtual machine from the list.
- 2 Click **Console** and select **Launch remote console** from the drop-down menu.
The VMware Remote Console opens as a stand-alone application for the selected virtual machine.

Managing a Guest Operating System in the VMware Host Client

With the VMware Host Client, you can manage the guest operating system of the virtual machine. You can install and upgrade VMware Tools, and you can also shut down, reboot, and change the configured guest operating system.

Shut Down and Restart a Guest Operating System by Using the VMware Host Client

Install VMware Tools on a virtual machine to be able to shut down and restart the guest operating system on that virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory and click a virtual machine in the list.
The virtual machine is displayed in the VMware Host Client inventory.
- 2 To shut down a virtual machine, right click the virtual machine in the VMware Host Client inventory, select **Guest OS** from the pop-up menu, and select **Shut down**.
- 3 To restart a virtual machine, right-click the virtual machine in the VMware Host Client inventory, select **Guest OS** from the drop-down menu, and select **Restart**.

Change the Guest Operating System in the VMware Host 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 configuration file of the virtual machine. 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 applies configuration defaults based on the type of guest operating system. Changing the guest operating system type setting affects the available ranges and recommendations of the virtual machine settings.

Prerequisites

Power off the virtual machine.

Procedure

- 1 In the VMware Host Client inventory, right-click the virtual machine and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **General Options**.
- 3 Select a guest operating system type and version.
- 4 Click **Save** to apply your changes.

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

Introduction to VMware Tools

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine.

VMware Tools enhances the performance of a virtual machine and makes possible many of the ease-of-use features in VMware products. For example, the following features are just some of the features that are available only if VMware Tools is installed:

- Significantly faster graphics performance and Windows Aero on operating systems that support Aero
- The Unity feature, which enables an application in a virtual machine to appear on the host desktop like any other application window
- Shared folders between host and guest file systems
- Copying and pasting text, graphics, and files between the virtual machine and the host or client desktop
- Improved mouse performance
- Synchronization of the clock in the virtual machine with the clock on the host or client desktop
- Scripting that helps automate guest operating system operations
- Runs pre-freeze and post-thaw quiescing scripts
- Enables capturing quiesced snapshots of guest operating systems

- Periodically collects and sends network, disk, and memory usage information from guest operating systems to ESXi hosts.
- Sends heartbeat information to each virtual machine every second and collects guest heartbeat information from guest operating systems. VMware HA uses the heartbeat information to determine virtual machine availability.
- Transports the OVF environment to guest operating systems using the guest OS environment variable *guestinfo.ovfEnv* that contains the XML document.
- Enables guest customization for virtual machines.

Although the guest operating system can run without VMware Tools, many VMware features are not available until you install VMware Tools. For example, if you do not have VMware Tools installed in your virtual machine, you cannot get heartbeat information from guest operating systems or cannot use the shutdown or restart options from the toolbar. You can only use the power options and you have to shut down your guest operating systems from each virtual machine console. You cannot use VMware Tools for connecting and disconnecting virtual devices, and shrinking virtual disks.

The installation procedure varies, depending on the operating system. For information about installing or upgrading VMware Tools on your guest operating systems, see the *Upgrading Virtual Machines* chapter. For instructions about installing VMware Tools, see the VMware Knowledge base article at <http://kb.vmware.com/kb/1014294>.

VMware highly recommends that you always run the latest version of VMware Tools. You can configure your virtual machine to automatically check for and apply VMware Tools upgrades each time you power on your virtual machines. For information about enabling automatic upgrade of VMware Tools on your virtual machines, see *vSphere Virtual Machine Administration*.

Installing VMware Tools

Although you can use guest operating systems without VMware Tools, many VMware features are not available unless you install VMware Tools. VMware Tools enhances the performance of the guest operating system of your virtual machines.

Installing VMware Tools is part of the process of creating new virtual machines. It is important to upgrade VMware Tools as updates become available. For information about creating virtual machines, see the *Virtual Machine Administration Guide*.

The installers for VMware Tools are ISO image files. An ISO image file looks like a CD-ROM to your guest operating system. Each type of guest operating system, including Windows, Linux, Solaris, FreeBSD, and NetWare, has an ISO image file. When you install or upgrade VMware Tools, the first virtual CD-ROM disk drive of the virtual machine temporarily connects to the VMware Tools ISO file of your guest operating system.

For information about installing or upgrading VMware Tools in Windows virtual machines, Linux virtual machines, Mac OS X virtual machines, Solaris virtual machines, NetWare virtual machines, or FreeBSD virtual machines, see *Virtual Machine Administration Guide*.

Install VMware Tools from the VMware Host Client

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance and management of the virtual machine.

You can install VMware Tools in one or more virtual machines by using the VMware Host Client.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Select a virtual machine from the list.
The virtual machine must be powered on to install VMware Tools.
- 3 Click **Actions**, select **Guest OS** from the drop-down menu, and select **Install VMware Tools**.

Upgrading VMware Tools

You can upgrade VMware Tools manually, or you can configure virtual machines to check for and install newer versions of VMware Tools.

The guest operating system checks the version of VMware Tools when you power on a virtual machine. The status bar of your virtual machine displays a message when a new version is available.

In Windows virtual machines, you can set VMware Tools to notify you when an upgrade is available. If this notification option is enabled, the VMware Tools icon in the Windows taskbar includes a yellow caution icon when a VMware Tools upgrade is available.

To install a VMware Tools upgrade, you can use the same procedure that you used for installing VMware Tools the first time. Upgrading VMware Tools means installing a new version.

For Windows and Linux guest operating systems, you can configure the virtual machine to automatically upgrade VMware Tools. Although the version check is performed when you power on the virtual machine, on Windows guest operating systems, the automatic upgrade occurs when you power off or restart the virtual machine. The status bar displays the message `Installing VMware Tools ...` when an upgrade is in progress.

Important After you upgrade VMware Tools on Linux guest operating systems, new network modules are available but are not used until you either restart the guest operating system or stop networking, unload and reload the VMware networking kernel modules, and restart networking. This behavior means that even if VMware Tools is set to automatically upgrade, you must restart or reload network modules to make new features available.

This strategy avoids network interruptions and allows you to install VMware Tools over SSH.

Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver makes the sleep mode available in guest OS power settings to adjust the sleep options. For example, you can use the sleep mode setting **Change when the computer sleeps** to configure your guest OS to automatically go to sleep mode after a certain time or prevent your guest OS from automatically switching to sleep mode after being idle for some time.

For vSphere virtual machines, you can use one of the following processes to upgrade multiple virtual machines at the same time.

- Log in to vCenter Server, select a host or cluster, and on the **Virtual Machines** tab specify the virtual machines on which to perform a VMware Tools upgrade.
- Use Update Manager to perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

Some features in a particular release of a VMware product might depend on installing or upgrading to the version of VMware Tools included in that release. Upgrading to the latest version of VMware Tools is not always necessary. Newer versions of VMware Tools are compatible with several host versions. To avoid unnecessary upgrades, evaluate whether the added features and capabilities are necessary for your environment.

Table 3-1. Virtual Machine Compatibility Options

Compatibility	Description
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0 and later.
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5 and later.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1 and later.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0 and 5.1.
ESX/ESXi 4.x and later	This virtual machine (hardware version 7) is compatible with ESX/ ESXi 4.x, ESXi 5.0, and ESXi 5.1.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESX 3.5, ESX/ESX 4.x, and ESXi 5.1. It is also compatible with VMware Server 1.0 and later. You cannot create a virtual machine with ESX/ESXi 3.5 compatibility on ESXi 5.0.

For more information, see the documentation for your specific VMware product.

Upgrade VMware Tools in the VMware Host Client

You can upgrade VMware Tools on a virtual machine by using the VMware Host Client.

Prerequisites

Power on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Select a virtual machine from the list.
- 3 Click **Actions**, select **Guest OS** from the drop-down menu, and select **Upgrade VMware Tools**.

Configuring a Virtual Machine in the VMware Host Client

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 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 the virtual machine, and VMware Tools settings.
Resources	Configure CPUs, CPU hyperthreading sources, memory, and disks.

Check the Hardware Version of a Virtual Machine in the VMware Host Client

You can check the hardware version of a virtual machine by looking at the virtual machine summary page.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.

The hardware version appears under the virtual machine name.

Change the Name of a Virtual Machine in the VMware Host Client

You can change the name of a virtual machine after you finish the creation process. 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

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 Click **VM Options**.
- 4 In the **VM Name** text box, enter a new name for the virtual machine.
- 5 Click **Save**.

View the Location of the Virtual Machine Configuration File in the VMware Host Client

You can view the location of the configuration files and the working files of a virtual machine by using the VMware Host Client.

This information is useful when you configure backup systems.

Prerequisites

Power off the virtual machine.


Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine and click **Edit Settings**.
- 3 Click the **VM Options** tab and expand **General Options**.
- 4 Record the location of the configuration files and the working files.
- 5 Click **Cancel** to exit the screen.

Configure the Virtual Machine Power States in the VMware Host Client

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the virtual machine power controls, or you can configure the controls to interact with the guest operating system. For example, you can configure the **Power off** control 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.

You cannot configure a **Power on** () action. This action powers on a virtual machine that is stopped, or starts a virtual machine and runs a script if the virtual machine is suspended and VMware Tools is installed and available. If VMware Tools is not installed, it starts the suspended virtual machine and does not run a script.

Prerequisites

- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, install VMware Tools on the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine from the list and select **Edit settings** from the drop-down menu.
- 3 On the **VM Options** tab, expand **VMware Tools**.

- 4 Select an option for the virtual machine **Power off** () control from the drop-down menu.

Option	Description
Power Off	Immediately stops the virtual machine. A Power Off action shuts down the guest operating system or powers off the virtual machine. A message indicates that the guest operating system might not shut down properly. Use this power off option only when necessary.
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. Soft power operations are possible only if the tools are installed in the guest operating system.
Default	Follows system settings. The current value of the system settings appears in parentheses.

- 5 Select an option for the **Suspend** () control from the drop-down menu.

Option	Description
Suspend	Pauses all virtual machine activity. When VMware Tools is installed and available, a suspend action runs a script and suspends the virtual machine. If VMware Tools is not installed, a Suspend action suspends the virtual machine without running a script.
Default	Follows system settings. The current value of the system settings appears in parentheses.

- 6 Select an option for the **Reset** () control from the drop-down menu.

Option	Description
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. If VMware Tools is not installed, a Reset action resets the virtual machine.
Restart Guest	Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.
Default	Follows system settings. The current value of the system settings appears in parentheses.

- 7 Click **Save**.

Edit the Configuration File Parameters in the VMware Host Client

To fix certain problems with your system, VMware documentation or a VMware Technical Support representative might instruct you to change or add virtual machine configuration parameters.

Important Changing or adding parameters when a system does not have problems might lead to decreased system performance and instability.

The following conditions apply:

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

Caution You must assign a value to configuration parameter keywords. If you do not assign a value, the keyword might receive a value of 0, false, or disable, which might result in a virtual machine that cannot power on.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **VM Options** tab, expand **Advanced**.
- 4 Click **Edit Configuration**.
- 5 (Optional) To add a parameter, click **Add Parameter** and enter a name and value for the parameter.
- 6 (Optional) To change a parameter, type a new value in the **Value** text box for that parameter.
- 7 Click **Save**.

Configure Autostart for a Virtual Machine in the VMware Host Client

Configure auto start options for a virtual machine to set up the virtual machine to start before or after the other virtual machines on the host.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine from the list.
- 3 Select **Autostart** from the pop-up menu and click an option to configure the auto start options for this virtual machine.

Option	Description
Increase priority	Increase the start priority of this virtual machine so it starts before other virtual machines.
Decrease priority	Decrease the start priority of this virtual machine so it starts after other virtual machines.

Upgrade Virtual Machine Compatibility by Using the VMware Host Client

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility level to make a virtual machine compatible with the latest version of ESXi running on the host.

For information about virtual machine hardware versions and compatibility, see *vSphere Virtual Machine Administration*.

Prerequisites

- Create a backup or snapshot of the virtual machines. See [Using Snapshots To Manage Virtual Machines](#).
- Upgrade VMware Tools. On virtual machines that run Microsoft Windows, if you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all .vmdk files are available to the ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machine is stored on VMFS3, VMFS5 or NFS datastores.
- Verify that the compatibility settings for the virtual machines are not set to the latest supported version.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See *vSphere Virtual Machine Administration*.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine from the list and select **Upgrade VM Compatibility** from the pop-up menu.
- 3 Select the latest supported version and click **Upgrade**.

Virtual CPU Configuration

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

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

CPU	The CPU or processor is the component of a computer system that performs the tasks required for computer programs to run, and is the primary element that performs the computer functions. CPUs contain cores.
CPU Socket	A CPU socket is a physical connector on a computer motherboard that connects to a single physical CPU. Some motherboards have multiple sockets and can connect multiple multicore processors (CPUs).
Core	A core contains 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 contain a number of compute units, each of which has a number of corelets. Unlike a traditional processor core, a corelet lacks a complete set of private, dedicated execution resources and 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, are referred to as corelets in VMware documentation 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 the 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)	Virtual SMP or vSphere Virtual Symmetric Multiprocessing is a feature that enables a single virtual machine to have multiple processors.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine depends on the hardware version number of the virtual machine, the number of logical CPUs on the host, 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. The number of logical cores is equal to twice the number of physical cores if hyperthreading is enabled.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this function might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.
- 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 6.0 and later to have up to 128 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 means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 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 the Number of Virtual CPUs in the VMware Host Client

You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hotplug is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

Virtual CPU hot add is supported for virtual machines with multicore CPU support and ESXi 5.0 and later compatibility. When the virtual machine is turned on and CPU hot add is enabled, you can hot add virtual CPUs to running virtual machines. The number of CPUs that you add must be a multiple of the number of cores that exist on each socket.

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 virtual CPU hot add is not enabled, turn off the virtual machine before adding virtual CPUs.
- To hot add multicore CPUs, verify that the virtual machine is compatible with ESXi 5.0 and later.
- Verify that you have the **Virtual Machine.Configuration.Change CPU Count** privilege.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand CPU, and select the number of cores from the **CPU** drop-down menu.
- 4 Select the number of cores per socket from the **Cores Per Socket** drop-down menu.
- 5 Click **Save**.

Allocate CPU Resources in the VMware Host Client

To manage workload demands, 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 or GHz.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz or GHz.
Shares	Each virtual machine is granted CPU shares. The more shares a virtual machine has, the more often it receives a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand **CPU**, and allocate CPU capacity for the virtual machine.

Option	Description
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.
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.

- 4 Click **Save**.

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 of a Virtual Machine in the VMware Host Client

You can reconfigure the amount of memory allocated to a virtual machine to enhance performance.

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 compatibility setting.

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 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.

The memory size must be a multiple of 4MB.

Table 3-2. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 6.0	ESXi 6.0 and later	4080GB
ESXi 5.5	ESXi 5.5 and later	1011GB
ESXi 5.1	ESXi 5.1 and later	1011GB
ESXi 5.0	ESXi 5.0 and later	1011GB
ESX/ESXi 4.x	ESX/ESXi 4.0 and later	255GB
ESX/ESXi 3.x	ESX/ESXi 3.5 and later	65532MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESX/ESXi 3.5 and later compatibility running on ESXi 5.0 is restricted to 65,532MB.

Prerequisites

Power off the virtual machine.

Verify that you have the **Virtual machine.Configuration.Memory** privilege on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand **Memory**.
- 4 In the **RAM** text box, type the amount of RAM to assign to the virtual machine or select one of the suggested values from the drop-down menu.
- 5 Select whether the memory is specified in MB or GB.
- 6 Click **Save**.

Allocate Memory Resources to a Virtual Machine in the VMware Host Client

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings. The host determines the appropriate amount of physical RAM to allocate to virtual machines based on these settings. You can assign a high or low shares value to a virtual machine, depending on its load and status.

The following user-defined settings affect the memory resource allocation of a virtual machine.

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. If the reservation cannot be met, the virtual machine will not turn on.
Shares	Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the greater share of host memory it receives. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the <i>vSphere Resource Management</i> documentation.

You cannot assign a reservation to a virtual machine that is larger than the virtual machine's configured memory. If you give a virtual machine a large reservation and reduce the virtual machine's configured memory size, the reservation is reduced to match the new configured memory size.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand **Memory**, and allocate the memory capacity for the virtual machine.

Option	Description
Reservation	Guaranteed memory allocation for this virtual machine.
Limit	Upper limit for this virtual machine's memory allocation. Select Unlimited to specify no upper limit.
Shares	The values Low , Normal , High , and Custom are compared to the sum of all shares of all virtual machines on the server.

- 4 Click **Save**.

Change Memory Hot Add Settings in the VMware Host Client

With memory hot add, you can add memory resources for a virtual machine while that virtual machine is turned on.

Enabling memory hot add produces extra memory overhead on the ESXi host for the virtual machine.

Prerequisites

- Power off the virtual machine.

- Verify that the virtual machine has a guest operating system that supports memory hot add capabilities.
- Verify that the virtual machine compatibility is ESXi 4.x and later.
- Verify that VMware Tools is installed.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand **Memory**, and select **Enable** to enable adding memory to the virtual machine while it is turned on.
- 4 Click **Save**.

Network Virtual Machine Configuration

ESXi networking features enable 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 enable communication between VMkernel services, such as 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.

Network Adapter Types

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.

The type of network adapters that are available depend on the following factors:

- The virtual machine compatibility, which depends on the host that created or most recently updated it.
- Whether the virtual machine compatibility has been updated to the latest version for the current host.
- The guest operating system.

The following NIC types are supported:

E1000E	Emulated version of the Intel 82574 Gigabit Ethernet NIC. E1000E is the default adapter for Windows 8 and Windows Server 2012.
E1000	Emulated version of the Intel 82545EM Gigabit Ethernet NIC, with drivers available in most newer guest operating systems, including Windows XP and later and Linux versions 2.4.19 and later.

Flexible	Identifies itself as a Vlan adapter when a virtual machine boots, but initializes itself and functions as either a Vlan or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlan adapter to the higher performance VMXNET adapter.
Vlan	Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.
VMXNET	Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.
VMXNET 2 (Enhanced)	Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ESXi 3.5 and later.
VMXNET 3	A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.
SR-IOV passthrough	<p>Representation of a virtual function (VF) on a physical NIC with SR-IOV support. The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary. This adapter type is suitable for virtual machines where latency might cause failure or that require more CPU resources.</p> <p>SR-IOV passthrough is available in ESXi 5.5 and later for guest operating systems Red Hat Enterprise Linux 6 and later, and Windows Server 2008 R2 with SP2. An operating system release might contain a default VF driver for certain NICs, while for others you must download and install it from a location provided by the vendor of the NIC or of the host.</p> <p>For information about assigning an SR-IOV passthrough network adapter to a virtual machine, see the <i>vSphere Networking</i> documentation.</p>

For network adapter compatibility considerations, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Network Adapters and Legacy Virtual Machines

Legacy virtual machines are virtual machines that are supported by the product in use, but are not current for that product. The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to correspond with an upgrade to a newer version of an ESXi host, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Change the Configuration of the Virtual Network Adapter in the VMware Host Client

You can configure the power-on connection setting, the MAC address, and the network connection of the virtual network adapter of 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 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 Click the **Virtual Hardware** tab and select the appropriate Network Adapter (NIC) from the hardware list.
- 4 (Optional) To connect the virtual NIC when the virtual machine is powered on, select **Connect at power on**.
- 5 Select an option for MAC address configuration.

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

- 6 Click **Save**.

Add a Network Adapter to a Virtual Machine in the VMware Host Client

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

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 Click the **Virtual Hardware** tab and click **Add network adapter**.
- 4 In the network connection panel, select either a network with a specific label or a legacy network.
- 5 (Optional) To configure the virtual NIC to connect when the virtual machine is powered on, select **Connect at power on**.
- 6 Click **Save**.

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.

To accelerate virtual machine performance, you can configure virtual machines to use vSphere Flash Read Cache™. For details about Flash Read Cache behavior, see the *vSphere Storage* documentation.

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.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

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.

Change the Virtual Disk Configuration in the VMware Host Client

If you run out of disk space, you can increase the size of the disk. You can change the virtual device node and the persistence mode of virtual disk configuration of a virtual machine.

Prerequisites

Power off the virtual machine.

Verify that you have the following privileges:

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine.Configuration.Extend virtual disk** on the virtual machine.
- **Datastore.Allocate space** on the datastore.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand the hard disk to view all disk options.
- 4 (Optional) To change the size of the disk, enter a new value in the text box and select the units from the drop-down menu.
- 5 (Optional) To change the way that disks are affected by snapshots, select a disk mode from the **Disk Mode** drop-down menu.

Option	Description
Dependent	Dependent disks are included in snapshots.
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 turn 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 turn off or reset the virtual machine.

- 6 Click **Save**.

Add a New Hard Disk to a Virtual Machine in the VMware Host Client

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

Prerequisites

- Verify that you are familiar with configuration options and caveats for adding virtual hard disks. See [Virtual Disk Configuration](#).
- Before you add disks larger than 2TB in size to a virtual machine, see *vSphere Virtual Machine Administration*.
- Verify that you have the **Virtual machine.Configuration.Add new disk** privilege on the destination folder or datastore.

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 (Optional) To delete an existing hard disk, move your pointer over the disk and click the **Remove** icon (X).

The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.

- 4 On the **Virtual Hardware** tab, select **Add hard disk** and select **New hard disk** from the drop-down menu.

The hard disk appears in the Virtual Hardware devices list.

- 5 Expand **New Hard disk**.
- 6 (Optional) Enter a value for the hard disk size and select the units from the drop-down menu.
- 7 Select the datastore location where you want to store the virtual machine files.
- 8 Select the format for the virtual machine disk.

Option	Description
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 requires. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

- 9 In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk.

Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.

- 10 If you selected **Custom**, enter a number of shares in the text box.

- 11 In the **Limit IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

This value is the upper limit of I/O operations per second allocated to the virtual disk.

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

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

- 13 (Optional) Select a disk mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent-Persistent	Disks in persistent mode behave like conventional physical computer disks. 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. The virtual disk returns to the same state every time you restart the virtual machine. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 14 Click **Save**.

Add an Existing Hard Disk to a Virtual Machine in the VMware Host Client

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

Prerequisites

- Verify that you are familiar with controller and virtual device node behavior for different virtual hard disk configurations.
- Verify that you have the **Virtual machine.Configuration.Add existing disk** privilege on the destination folder or datastore.

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add hard disk** and select **Existing hard disk** from the drop-down menu.
- 4 (Optional) To delete an existing hard disk, move your pointer over the disk and click the **Remove** icon (**X**).

The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.

- 5 In the Datastore column, expand a datastore, select a virtual machine folder, and select the disk to add.

The disk file appears in the Contents column. The **File type** menu shows the compatibility file types for this disk.

- 6 Click **Select** and click **Save** to add the existing hard disk.

Use Disk Shares to Prioritize Virtual Machines in the VMware Host 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 level of access that virtual machines have to resources. Disk shares distinguish high-priority from low-priority virtual machines.

You can allocate the I/O bandwidth of the host to the virtual hard disks of a virtual machine. You cannot pool disk I/O across a cluster.

The shares value represents the relative metric for controlling disk bandwidth to all virtual machines.

Disk shares are relevant only within a given 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 limit for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand the hard disk to view the disk options.
- 4 In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual machine.
- 5 If you selected **Custom**, enter a number of shares in the text box.

- 6 In the **Limit - IOPs** text box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.
- 7 Click **Save**.

Virtual Machine Controller Configuration in the VMware Host Client

In the VMware Host Client, you can add various controllers to virtual machines, such as USB controllers, SCSI controllers, Paravirtual SCSI controllers, and SATA controllers. You can also change the SCSI Bus sharing configuration and the SCSI controller type.

Add a USB Controller to a Virtual Machine in the VMware Host Client

USB controllers can be added to virtual machines to support USB passthrough from an ESXi host or from a client computer to a virtual machine.

You can add one virtual xHCI controller, one virtual EHCI controller, and one virtual UHCI controller per virtual machine. With Hardware Version 11, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.0 ports and four logical USB 2.0 ports).

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 3-3. 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 3.0, 2.0, and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

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 3.0, 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 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, click **Add other device**, and click **USB Controller** from the drop-down menu.

The new USB controller appears at the bottom of the Virtual Hardware device list.

- 4 Expand **New USB Controller** to change the USB controller type.
If compatibility errors appear, fix them before you add the controller.
- 5 Click **Save**.

What to do next

Add one or more USB devices to the virtual machine.

Add SCSI Controllers in the VMware Host Client

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 creates a new SCSI controller.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add hard disk** and select **New hard disk** from the drop-down menu.
- 4 Expand the hard disk to view all options.
- 5 In the **Virtual Device Node** section, select an unused SCSI Bus number from the drop-down menu.
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.
- 6 Click **Save**.

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

Change the SCSI Bus Sharing Configuration in the VMware Host Client

You can set the type of SCSI bus sharing for a virtual machine and indicate whether to share the SCSI bus. 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 only if the virtual machine is on an ESXi host.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, expand the SCSI Controller that you want to edit.
- 4 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.

- 5 Click **Save**.

Change the SCSI Controller Type in the VMware Host Client

You can attach virtual disks and RDMS to virtual machines by configuring virtual SCSI controller on the virtual machines.

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 have BusLogic adapter as their default controller.

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.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 Click the **Virtual Hardware** tab and expand a SCSI controller.
- 4 Select a SCSI controller type from the drop-down menu.
- 5 Click **Save**.

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 in the VMware Host Client

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

VMware Paravirtual SCSI controllers are best suited for environments, especially SAN environments, that run 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.
- Familiarize yourself with VMware Paravirtual SCSI limitations. See *vSphere Virtual Machine Administration*.
- To access boot disk devices attached to a VMware Paravirtual SCSI 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 must create a virtual machine with an LSI Logic controller and install VMware Tools.

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, click **Add other device** and select **SCSI Controller** from the drop-down menu.

The new SCSI Controllers appears in the Hardware list.

- 4 Click on the **New SCSI Controller** and select **VMware Paravirtual** from the drop-down menu.
- 5 Click **Save**.

Add a SATA Controller to a Virtual Machine in the VMware Host Client

If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you assign the devices to different controllers, you can improve performance and avoid data traffic congestion. You can also add controllers if you need to exceed the thirty-device limit for a single controller.

You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.

Not all guest operating systems support AHCI SATA controllers. Typically, when you create virtual machines with ESXi 5.5 and later compatibility and Mac OS X guest operating systems, a SATA controller is added by default for the virtual hard disk and CD/DVD-ROM devices. Most guest operating systems, including Windows Vista and later, have a default SATA controller for CD/DVD-ROM devices. For verification, see the appropriate *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.5 and later.
- Verify that you are familiar with storage controller behavior and limitations. See *vSphere Virtual Machine Administration*.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.
- Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add other device**, and select **SATA Controller** from the drop-down menu.

The SATA controller appears in the hardware list.

- 4 Click **Save**.

Other Virtual Machine Device Configuration in the VMware Host Client

In addition to configuring virtual machine CPU and Memory, and adding hard disks and virtual network adapters, you can also add and configure virtual hardware, such as DVD/CD-ROM drives, floppy drives, and SCSI devices.

Add a CD or DVD Drive to a Virtual Machine in the VMware Host Client

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

If you want to add a CD/DVD drive that is backed up 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.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add other device** and select **CD/DVD Drive** from the drop-down menu.
- 4 Expand **CD/DVD drive** and select an option.

Option	Description
Use physical drive	<ol style="list-style-type: none"> a Select Client Device as the location. b From the Device Mode drop-down menu, select Emulate CD-ROM or Passthrough CD-ROM.
Use ISO Image	<ol style="list-style-type: none"> a Select Datastore ISO File as the location. b 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 to connect when the virtual machine starts, deselect **Connect at power on**.
- 6 Select the virtual device node that the drive uses in the virtual machine.
- 7 Click **Save**.

Add a Floppy Drive to a Virtual Machine in the VMware Host 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 up by a physical floppy drive on the host.

Prerequisites

- Power off the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add other device** and select **Floppy Drive** from the drop-down menu.

The Floppy drive appears in the hardware list.

- 4 Expand **Floppy drive** and select the type of device you want to use.

Option	Description
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system from which you access the VMware Host Client .
Use existing floppy image	<ol style="list-style-type: none"> a Select this option to connect the virtual device to an existing image of a floppy drive on a datastore accessible to the host . b Click Browse and select the floppy image.

- 5 (Optional) Select **Connect at power on** to configure the device to connect when the virtual machine powers on.
- 6 Click **Save**.

Parallel and Serial Port Configuration in the VMware Host Client

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.

Add a Serial Port to a Virtual Machine in the VMware Host 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 a Virtual Serial Port Concentrator (vSPC) URI to connect a serial port over the network.

Prerequisites

- Familiarize yourself with the different media types that the port can access, vSPC connections, and any conditions that might apply. See *vSphere Virtual Machine Administration*.

- To connect a serial port over a network, add a Firewall rule set. See *vSphere Virtual Machine Administration*.
- Required privilege: **Virtual Machine .Configuration.Add or Remove Device**
Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add other device** and select **Serial Port**.
The Serial Port appears in the hardware list.
- 4 In the hardware list, expand the serial port and select the type of media port to access.

Option	Description
Use output file	Browse to the location of the file on the host to store the output of the virtual serial port.
Use physical serial port	Select the port from the drop-down menu.
Use named pipe	<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.
Use network	<ol style="list-style-type: none"> a From the Direction drop-down menu, select Server or Client. b Type the port URI. The URI is the remote end of the serial port to which the serial port of the virtual machine should connect. 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) Deselect **Connect at power on** if you do not want the parallel port device to connect when the virtual machine powers on.
- 6 Click **Save**.

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 Parallel Port to a Virtual Machine in the VMware Host Client

To connect peripheral devices to virtual machines, such as printers and scanners, you can use a parallel port. You send the output of such devices to a file on the host computer.

Note To add a parallel port to a virtual machine that runs on an ESXi 4.1 or earlier host, you can also select to send output to a physical parallel port on the host. This option is not available with ESXi 5.0 and later host versions.

Prerequisites

- Power off the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
- 3 On the **Virtual Hardware** tab, select **Add other device** and select **Parallel Port**.
The parallel port appears in the hardware list.
- 4 In the virtual hardware list, expand the parallel port and click **Browse** to locate a folder to create the file in.
- 5 Choose a folder from the list and click **Select**.
The file path appears in the **Connection** text box.
- 6 (Optional) Select **Connect at power on** to configure the device to connect when the virtual machine powers on.
- 7 Click **Save**.

Managing Virtual Machines in the VMware Host Client

After creating a virtual machine in the VMware Host Client, you can perform different management tasks on the virtual machine, including deleting the virtual machine from the host, remove the virtual machine from a datastore, registering it back on a datastore, and so on. You can also return the virtual machine to the host.

Access a Virtual Machine in the VMware Host Client

You can access the virtual machines on the host that you are logged in to, to configure the virtual machine hardware and options, to perform administrative tasks, and to perform basic troubleshooting tasks.

To display a virtual machine in the VMware Host Client inventory, power on the virtual machine.

Procedure

- ◆ To access the virtual machines that are available on the host that you are logged in to, click **Virtual Machines** in the VMware Host Client inventory.

The list of available virtual machines is displayed under **Virtual Machines**.

You can now edit the virtual machine settings and perform different administrative and troubleshooting tasks on the virtual machines in the list.

Use Virtual Machine Column Configuration in the VMware Host Client

When you view virtual machines in the VMware Host Client, you can configure what information is displayed by including and excluding columns such as status, provisioned space, host name, host CPU, and so on.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click **Columns** and select the information that you want to display or hide in the virtual machine panel.

Remove Virtual Machines from a Host in the VMware Host Client

You can unregister a virtual machine if you want to keep it on the datastore, but you no longer want the VMware Host Client inventory to display the virtual machine.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine from the list and select **Unregister**.
- 3 To confirm that you want to remove the virtual machine from the inventory, click **Yes**.

The host removes the virtual machine from the inventory and no longer tracks its condition.

Remove Virtual Machines from the Datastore in the VMware Host Client

Remove unnecessary virtual machines from the VMware Host Client inventory to free space on the datastore. Removing a virtual machine from the host deletes all virtual machine files from the datastore, including the configuration file and virtual disk files.

Prerequisites

- Power off the virtual machine.

- Verify that the virtual machine does not share the disk with another virtual machine. If two virtual machines are sharing the same disk, the disk files are not deleted.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine from the list and select **Delete** from the drop-down menu.
- 3 Click **Delete**.

Register a Virtual Machine in the VMware Host Client

If you remove a virtual machine or template from a host but do not remove it from the host datastore, you can return it to the host's inventory.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory.
- 2 Right-click a datastore from the list and click **Register a VM**.
- 3 Select the virtual machine you want to register from the list and click **Register**.

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, the virtual machine is not affected and only an image of the virtual machine in a given state is copied and stored. 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 be able to perform many types 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 making changes to a virtual machine in the snapshot tree.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the Snapshot Manager of the VMware Host Client. These operations enable you to 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 state of a virtual machine 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 the disks added or changed after you take 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. Snapshots in the hierarchy have parent to child relationships. In linear processes, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshot. 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 of a virtual machine taken after the parent snapshot. Each child snapshot contains 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 by 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.

Snapshot Files

When you take a snapshot, you capture the state of the virtual machine settings and the virtual disk. If you are taking a memory snapshot, you also capture the memory state of the virtual machine. These states are saved to files that reside with the virtual machine's base files.

Snapshot Files

A snapshot consists of files that are stored on a supported storage device. A Take Snapshot operation creates `.vmdk`, `-delta.vmdk`, `.vmsd`, and `.vmsn` files. By default, the first and all delta disks are stored with the base `.vmdk` file. The `.vmsd` and `.vmsn` files are stored in the virtual machine directory.

Delta disk files

A `.vmdk` file to which the guest operating system can write. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken. When you take a snapshot, the state of the virtual disk is preserved, which prevents the guest operating system from writing to it, and a delta or child disk is created.

A delta disk has two files, including a descriptor file that is small and contains information about the virtual disk, such as geometry and child-parent relationship information, and a corresponding file that contains the raw data.

The files that make up the delta disk are referred to as child disks or redo logs. A child disk is a sparse disk. Sparse disks use the copy-on-write mechanism, in which the virtual disk contains no data in places, until copied there by a write operation. This optimization saves storage space. A grain is the unit of measure in which the sparse disk uses the copy-on-write mechanism. Each grain is a block of sectors that contain virtual disk data. The default size is 128 sectors or 64KB.

Flat file

A `-flat.vmdk` file that is one of two files that comprises the base disk. The flat disk contains the raw data for the base disk. This file does not appear as a separate file in the Datastore Browser.

Database file

A `.vmsd` file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager. This file contains line entries, which define the relationships between snapshots and between child disks for each snapshot.

Memory file

A `.vmsn` file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state. With nonmemory snapshots, you can only revert to a turned off virtual machine state. Memory snapshots take longer to create than nonmemory snapshots. The time the ESX host takes to write the memory onto the disk is relative to the amount of memory the virtual machine is configured to use.

A **Take Snapshot** operation creates `.vmdk`, `-delta.vmdk`, `vmsd`, and `vmsn` files.

File	Description
<code>vmname-number.vmdk</code> and <code>vmname-number-delta.vmdk</code>	<p>Snapshot file that represents the difference between the current state of the virtual disk and the state that existed at the time the previous snapshot was taken.</p> <p>The filename uses the following syntax, <code>S1vm-000001.vmdk</code> where <code>S1vm</code> is the name of the virtual machine and the six-digit number, <code>000001</code>, is based on the files that already exist in the directory. The number does not consider the number of disks that are attached to the virtual machine.</p>
<code>vmname.vmsd</code>	<p>Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.</p>
<code>vmname.Snapshotnumber.vmsn</code>	<p>Memory state of the virtual machine at the time you take the snapshot. The file name uses the following syntax, <code>S1vm.snapshot1.vmsn</code>, where <code>S1vm</code> is the virtual machine name, and <code>snapshot1</code> is the first snapshot.</p> <p>Note A <code>.vmsn</code> file is created each time you take a snapshot, regardless of the memory selection. A <code>.vmsn</code> file without memory is much smaller than one with memory.</p>

Snapshot Limitations

Snapshots can affect virtual machine performance and do not support some disk types or virtual machines configured with bus sharing. Snapshots are useful as short-term solutions for capturing point-in-time virtual machine states and are not appropriate for long-term virtual machine backups.

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- Virtual machines with independent disks must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.
- Snapshots are not supported with PCI vSphere Direct Path I/O devices.
- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.
- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected in the case of hardware failure.
- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power-on. Do not run production virtual machines from snapshots on a permanent basis.
- If a virtual machine has virtual hard disks larger than 2TBs, snapshot operations can take significantly longer to finish.

Taking Snapshots of a Virtual Machine

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. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

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 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 are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

If the virtual machine is powered off or VMware Tools is 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.

Take a Snapshot in the VMware Host 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. To take a snapshot of a suspended 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, snapshots that capture the memory state of a virtual machine take 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 stores on the disk during a restore operation.

Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.

Note If you take a snapshot of a Dynamic Disk (Microsoft-specific disk type), the snapshot technology preserves the quiesced state of the file system, but does not preserve the quiesced state of the application.

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.
- Verify that you have the **Virtual machine.Snapshot management. Create snapshot** privilege on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click a virtual machine from the list, select **Snapshots**, and select **Take snapshot** from the pop-up menu.
- 3 Enter a name for the snapshot.
- 4 (Optional) Type a description for the snapshot.
- 5 (Optional) Select the **Snapshot the virtual machine's memory** check box to capture the memory of the virtual machine.
- 6 (Optional) Deselect **Snapshot the virtual machine's memory** and select **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.

Quiesce the virtual machine files only when the virtual machine is powered on and you do not want to capture the virtual machine's memory.
- 7 Click **OK**.

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 Latest Snapshot Restores the parent snapshot, one level up in the hierarchy from the **You are Here** position. **Revert to Latest Snapshot** activates the parent snapshot of the current state of the virtual machine.

Revert 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 3-4. 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.

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 VMware Host Client

Revert to a snapshot to restore the virtual machine to the state of the snapshot.

Prerequisites

Verify that you have the **Virtual machine.Snapshot management.Revert to snapshot** privilege on the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine in the list, select **Snapshots**, and select **Revert to snapshot** from the pop-up menu.

Note The current state of the virtual machine will be lost unless you save it in a snapshot.

- 3 Click **Revert** to revert the virtual machine to the most recent snapshot.

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 does not change the virtual machine or other snapshots. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes all the data from the delta disk that contains the information about the deleted snapshot to the parent disk. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

To delete a snapshot, a lot of information needs to be read and written to a disk. This 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 amount of data that the guest operating system writes to the virtual disks after you take 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.

Failure of disk consolidation can reduce the performance of virtual machines. You can check whether any virtual machines require separate consolidation operations by viewing a list. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see *vSphere Virtual Machine Administration*.

Delete

Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes that occur between the state of the snapshot and the previous 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 the changes that occur between snapshots and the 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 if, for example, an update or installation fails, first use the **Restore** 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 VMware Host Client

You can use the Snapshot Manager to delete a single snapshot or all snapshots in a tree.

Be careful not to accidentally delete a snapshot that you need. 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.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine in the list, select **Snapshots** from the pop-up menu and click **Manage Snapshots**.
- 3 Click the snapshot that you want to delete and click **Delete**.
- 4 Click **Remove**.
- 5 Click **Close** to navigate out of the Snapshot Manager.

Managing Snapshots with the VMware Host Client

You can review all snapshots for your virtual machines and use the Snapshot Manager to manage the snapshots.

After you take a snapshot, you can right-click a virtual machine and click **Revert to snapshot** to restore the virtual machine to the state of the snapshot at any time.

If you have a series of snapshots, you can use the Snapshot Manager to restore any parent or child snapshot. Subsequent child snapshots that you take from the restored snapshot create a branch in the snapshot tree. Use the Snapshot Manager to delete a snapshot from the tree.

Table 3-5. Snapshot Manager

Option	Description
Snapshot tree	Displays all snapshots for the virtual machine.
You are here icon	The You are here icon represents the current and active state of the virtual machine. The Restore , Delete , and Edit actions are disabled for the You are here state.
Take, Restore, Delete, Edit	Snapshot options.
Details	Shows the snapshot name and description, the date you created the snapshot. The Console shows the power state of the virtual machine when a snapshot was taken. The Name, Description, and Created text boxes are blank if you do not select a snapshot.

Monitoring a Virtual Machine in the VMware Host Client

You can monitor various performance aspects and keep track of the actions that take place on virtual machines that you create in the VMware Host Client.

View Virtual Machine Performance Charts in the VMware Host Client

You can view line charts with information about the resource usage of virtual machines that you create in the VMware Host Client.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.
- 3 Expand the virtual machine in the VMware Host Client inventory and click **Monitor**.
- 4 Click **Performance**.
- 5 To view the virtual machine resource usage for the last hour, select an option from the drop-down menu.
 - To view the percentage of CPU that the virtual machine used during the last hour, select **CPU usage**.
 - To view the memory that the host consumed during the last hour, select **Memory usage**.

View Virtual Machine Events in the VMware Host Client

Events are records of the actions that a user performs on a virtual machine. When you create a virtual machine in the VMware Host Client, you can view the events associated with the virtual machine.

Prerequisites

Required privilege: **Read only**.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.
- 3 Expand the virtual machine in the VMware Host Client inventory and click **Monitor**.
- 4 Click **Events**.

A list of all virtual machine events is displayed.
- 5 (Optional) Click an event from the list to view event details.
- 6 (Optional) Use the filter controls above the list to filter the list.
- 7 (Optional) Click a column heading to sort the list.

View Virtual Machine Tasks in the VMware Host Client

When you create a virtual machine in the VMware Host Client, you can view all virtual machine tasks and information about the task target, initiator, queue time, start time, result, and time of completion.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.
- 3 Expand the virtual machine in the VMware Host Client inventory and click **Monitor**.
- 4 Click **Tasks**.
- 5 (Optional) Click on a task from the list to view task details.
- 6 (Optional) Use the filter controls above the list to filter the list.
- 7 (Optional) Click a column heading to sort the list.

View Virtual Machine Log Browser in the VMware Host Client

Generate and monitor logs for the host that you are managing by using the VMware Host Client. Use the logs to diagnose and troubleshoot various issues with your host environment.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.
- 3 Expand the virtual machine in the VMware Host Client inventory and click **Monitor**.
- 4 Click **Logs**.
- 5 (Optional) Click **Generate support bundle** to consolidate all the logs for troubleshooting.
- 6 Right-click a log from the list and select **Open in new window** to view the log.

View Virtual Machine Notifications in the VMware Host Client

You can view virtual machine notifications and information about related tasks, which you can perform, for virtual machines that you create in the VMware Host Client.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Click a virtual machine from the list.
- 3 Expand the virtual machine in the VMware Host Client inventory and click **Monitor**.
- 4 Click **Notifications**.

A list with all virtual machine notifications is displayed.

- 5 (Optional) Click on a notification to view details.
- 6 (Optional) Click on a notification and click **Actions** to view suggested tasks.

Managing Storage in the VMware Host Client

4

When you connect to an ESXi host by using the VMware Host Client, you can perform different storage management tasks on the ESXi host, including configuring adapters, creating datastores, and viewing storage device information.

This chapter includes the following topics:

- [Working with Datastores in the VMware Host Client](#)
- [View Storage Adapters in the VMware Host Client](#)
- [Managing Storage Devices in the VMware Host Client](#)
- [Monitoring Storage in the VMware Host Client](#)
- [Performing Storage Refresh and Rescan Operations in the VMware Host Client](#)

Working with Datastores in the VMware Host Client

Datastores are logical containers, similar to file systems, that contain specific information of each storage device and provide a uniform model for storing virtual machine files. You can also use datastores to store ISO images, virtual machine templates, and floppy images.

Depending on the type of storage you use, datastores can be of the following types:

- Virtual Machine File System (VMFS)
- Network File System (NFS)

You can increase datastore capacity after you create a datastore but only if it is a VMFS datastore.

View Datastore Information in the VMware Host Client

Use the VMware Host Client to display the datastores available to the hosts and analyze their properties.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 To view the details for a specific datastore, select the datastore from the list.

Creating a VMFS Datastore in the VMware Host Client

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that your host detects, including Fibre Channel, iSCSI, and local storage devices.

1 Start the VMFS Datastore Creation Process in the VMware Host Client

You can use the **New datastore** wizard to create datastores in the VMware Host Client.

2 Select a Method for Adding a New Datastore to the Host in the VMware Host Client

You can use the Select creation type page of the **New datastore** wizard to choose whether you want to create a new VMFS datastore, extend an existing one, or mount an NFS datastore.

3 Select a Device on Which to Add a VMFS Datastore in the VMware Host Client

Select where to create a VMFS datastore in the VMware Host Client.

4 Select Partitioning Options in the VMware Host Client

Use the Select partitioning options page of the **New datastore** wizard to select how you would like to partition the device.

5 Complete Datastore Creation Process in the VMware Host Client

In the Ready to complete page of the **New datastore** wizard, you can review your configuration selections for the new datastore.

Start the VMFS Datastore Creation Process in the VMware Host Client

You can use the **New datastore** wizard to create datastores in the VMware Host Client.

Prerequisites

Install and configure any adapters that your storage requires. Rescan the adapters to discover newly added storage devices.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **New datastore**.

The **New datastore** wizard opens.

Select a Method for Adding a New Datastore to the Host in the VMware Host Client

You can use the Select creation type page of the **New datastore** wizard to choose whether you want to create a new VMFS datastore, extend an existing one, or mount an NFS datastore.

Procedure

- ◆ Select a creation type for the new datastore and click **Next**.

Option	Description
Create new VMFS datastore	Creates a new VMFS datastore on a local disk device.
Increase the size of an existing datastore	Increases the size of an existing datastore by adding a new extent on another disk.
Mount NFS datastore	Creates a new datastore by mounting a remote NFS volume.

Select a Device on Which to Add a VMFS Datastore in the VMware Host Client

Select where to create a VMFS datastore in the VMware Host Client.

The following procedure applies if you want to create a new VMFS datastore.

Procedure

- 1 Enter a name for the new datastore.
- 2 Select a device to add the datastore to and click **Next**.

The list contains only devices that have enough available space.

Select Partitioning Options in the VMware Host Client

Use the Select partitioning options page of the **New datastore** wizard to select how you would like to partition the device.

Procedure

- 1 Click the **Select partitioning scheme** drop-down menu and select an option.

Option	Description
Use Full Disk	It shows you all the free space that is available on the device.
Custom	Click the Free space bar and use the horizontal scroller to partition the device.

- 2 Click **Next**.

Complete Datastore Creation Process in the VMware Host Client

In the Ready to complete page of the **New datastore** wizard, you can review your configuration selections for the new datastore.

Procedure

- ◆ Review the configuration selections summary and click **Finish**.

Increasing VMFS Datastore Capacity

If your VMFS datastore requires more space, increase the datastore capacity. You can dynamically increase the capacity by growing a datastore extent or by adding a new extent.

Use one of the following methods to increase a datastore capacity:

- Dynamically grow any expandable datastore extent, so that it fills the available adjacent capacity. The extent is considered expandable when the underlying storage device has free space immediately after the extent.
- Dynamically add a new extent. The datastore can span over up to 32 extents with the size of each extent of more than 2TB, yet appear as a single volume. 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.

Note Datastores that only support hardware assisted locking, also called atomic test and set (ATS) mechanism cannot span over non-ATS devices. For more information, see [VMFS Locking Mechanisms](#).

Increase an Existing VMFS Datastore in the VMware Host Client

When you need to add virtual machines to a datastore, or when the virtual machines running on a datastore require more space, you can dynamically increase the capacity of a VMFS datastore.

If a shared datastore has powered on virtual machines and becomes 100% full, you can increase the datastore's capacity only from the host that the powered on virtual machines are registered on.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **New datastore**.
- 3 Click **Increase the size of an existing VMFS datastore** and click **Next**.

Select the Datastore You Want to Increase in the VMware Host Client

Review the capacity and the available space on your datastores and choose which datastore you want to increase.

Procedure

- ◆ From the list of datastores, click the datastore that you want to increase and click **Next**.

Select a Device on Which to Create a New VMFS Partition in the VMware Host Client

Before you can increase an existing datastore in the VMware Host Client, select a device to create the new VMFS partition on.

Procedure

- ◆ Select a device from the list of unclaimed devices and click **Next**.

Select Partitioning Options in the VMware Host Client

Use the Select partitioning options page of the **New datastore** wizard to select how you would like to partition the device.

Procedure

- 1 Click the **Select partitioning scheme** drop-down menu and select an option.

Option	Description
Use Full Disk	It shows you all the free space that is available on the device.
Custom	Click the Free space bar and use the horizontal scroller to partition the device.

- 2 Click **Next**.

Complete Datastore Increase Process in the VMware Host Client

In the Ready to complete page of the **New datastore** wizard, you can review your configuration selections for the datastore that you want to increase.

Procedure

- ◆ Review the configuration selections summary and click **Finish**.

Mounting a Network File System Datastore in the VMware Host Client

With the VMware Host Client, you can create a Network File System (NFS) datastore to store virtual disks and to use as a central repository for ISO images, virtual machines, and so on.

1 [Understanding Network File System Datastores](#)

An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it for its storage needs. vSphere supports versions 3 and 4.1 of the NFS protocol.

2 [NFS Storage Guidelines and Requirements](#)

When using NFS storage, you must follow specific configuration, networking, and NFS datastore guidelines.

3 [Mount an NFS Datastore in the VMware Host Client](#)

Use the **New datastore** wizard to mount a Network File System (NFS) datastore in the VMware Host Client.

4 [Provide NFS Details](#)

Before you mount an NFS datastore in the VMware Host Client, you must specify a name, a server, and a share.

5 Complete the NFS Datastore Mounting Process in the VMware Host Client

In the Ready to complete page you can review your configuration selections for your NFS datastore.

Understanding Network File System Datastores

An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it for its storage needs. vSphere supports versions 3 and 4.1 of the NFS protocol.

Typically, the NFS volume or directory is created by a storage administrator and is exported from the NFS server. The NFS volume is not required to be formatted with a local file system, such as VMFS. You can mount the volume directly on ESXi hosts and use it to store and boot virtual machines in the same way that you use VMFS datastores.

In addition to storing virtual disks on NFS datastores, you can use NFS as a central repository for ISO images, virtual machine templates, and so on. If you use the datastore for ISO images, you can connect the virtual machine's CD-ROM device to an ISO file on the datastore and install a guest operating system from the ISO file.

ESXi supports the following storage capabilities on most NFS volumes:

- vMotion and Storage vMotion
- High Availability (HA) and Distributed Resource Scheduler (DRS)
- Fault Tolerance (FT) and Host Profiles

Note NFS 4.1 does not support legacy Fault Tolerance.

- ISO images, which are presented as CD-ROMs to virtual machines
- Virtual machine snapshots
- Virtual machines with large capacity virtual disks, or disks greater than 2TB. Virtual disks created on NFS datastores are thin-provisioned by default, unless you use hardware acceleration that supports the Reserve Space operation. NFS 4.1 does not support hardware acceleration. For information, see [Hardware Acceleration on NAS Devices](#).

NFS Storage Guidelines and Requirements

When using NFS storage, you must follow specific configuration, networking, and NFS datastore guidelines.

NFS Server Configuration Guidelines

- Make sure that NFS servers you use are listed in the *VMware HCL*. Use the correct version for the server firmware.
- When configuring NFS storage, follow the recommendation of your storage vendor.
- Ensure that the NFS volume is exported using NFS over TCP.

- Make sure that the NFS server exports a particular share as either NFS 3 or NFS 4.1, but does not provide both protocol versions for the same share. This policy needs to be enforced by the server because ESXi does not prevent mounting the same share through different NFS versions.
- NFS 3 and non-Kerberos NFS 4.1 do not support the delegate user functionality that enables access to NFS volumes using nonroot credentials. If you use NFS 3 or non-Kerberos NFS 4.1, ensure that each host has root access to the volume. Different storage vendors have different methods of enabling this functionality, but typically this is done on the NAS servers by using the `no_root_squash` option. If the NAS server does not grant root access, you might still be able to mount the NFS datastore on the host. However, you will not be able to create any virtual machines on the datastore.
- If the underlying NFS volume, on which files are stored, is read-only, make sure that the volume is exported as a read-only share by the NFS server, or configure it as a read-only datastore on the ESXi host. Otherwise, the host considers the datastore to be read-write and might not be able to open the files.

NFS Networking Guidelines

- For network connectivity, the host requires a standard network adapter.
- ESXi supports Layer 2 and Layer 3 Network switches. If you use Layer 3 switches, ESXi hosts and NFS storage arrays must be on different subnets and the network switch must handle the routing information.
- A VMkernel port group is required for NFS storage. You can create a new VMkernel port group for IP storage on an already existing virtual switch (vSwitch) or on a new vSwitch when it is configured. The vSwitch can be a vSphere Standard Switch (VSS) or a vSphere Distributed Switch (VDS).
- If you use multiple ports for NFS traffic, make sure that you correctly configure your virtual switches and physical switches. For information, see the *vSphere Networking* documentation.
- NFS 3 and non-Kerberos NFS 4.1 support IPv4 and IPv6.

NFS Datastore Guidelines

- To use NFS 4.1, upgrade your vSphere environment to version 6.x. You cannot mount an NFS 4.1 datastore to hosts that do not support version 4.1.
- You cannot use different NFS versions to mount the same datastore. NFS 3 and NFS 4.1 clients do not use the same locking protocol. As a result, accessing the same virtual disks from two incompatible clients might result in incorrect behavior and cause data corruption.
- NFS 3 and NFS 4.1 datastores can coexist on the same host.
- vSphere does not support datastore upgrades from NFS version 3 to version 4.1.
- When you mount the same NFS 3 volume on different hosts, make sure that the server and folder names are identical across the hosts. If the names do not match, the hosts see the same NFS version 3 volume as two different datastores. This error might result in a failure of such features as vMotion. An example of such discrepancy is entering `filer` as the server name on one host and `filer.domain.com` on the other. This guideline does not apply to NFS version 4.1.

- If you use non-ASCII characters to name datastores and virtual machines, make sure that the underlying NFS server offers internationalization support. If the server does not support international characters, use only ASCII characters, or unpredictable failures might occur.

Mount an NFS Datastore in the VMware Host Client

Use the **New datastore** wizard to mount a Network File System (NFS) datastore in the VMware Host Client.

Prerequisites

Because NFS requires network connectivity to access data on remote servers, before configuring NFS, you must first configure VMkernel networking.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **New datastore**.
The **New datastore** wizard opens.
- 3 Click **Mount NFS datastore** and click **Next**.

Provide NFS Details

Before you mount an NFS datastore in the VMware Host Client, you must specify a name, a server, and a share.

Procedure

- 1 Enter a name for the NFS datastore.
- 2 Enter the NFS server 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, the hosts detect the same NFS volume as two different datastores. This might result in a failure of features such as vMotion. An example of such discrepancy is if you enter **filer** as the server name on one host and **filer.domain.com** on the other.

- 3 Specify the NFS share.
- 4 Click **Next**

Complete the NFS Datastore Mounting Process in the VMware Host Client

In the Ready to complete page you can review your configuration selections for your NFS datastore.

Procedure

- ◆ Review the settings for the NFS datastore and click **Finish**.

Unmount a Datastore in the VMware Host Client

When you unmount a datastore in the VMware Host Client, it remains intact, but you can no longer view it in the inventory of the host that you manage. The datastore continues to appear on other hosts that it remains mounted on.

Do not perform any configuration operations that might result in I/O to the datastore while the unmount is in progress.

Prerequisites

Note Make sure that the datastore is not used by vSphere HA heartbeating. vSphere HA heartbeating does not prevent you from unmounting the datastore. However, if the datastore is used for heartbeating, unmounting it might cause the host to fail and restart all active virtual machines.

Before unmounting a datastore, also make sure that the following prerequisites are met:

- No virtual machines reside on the datastore.
- The datastore is not managed by Storage DRS.
- Storage I/O control is disabled for this datastore.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Right-click the datastore to unmount from the list and click **Unmount**.
- 3 Confirm that you want to unmount the datastore.

Unmounting or Removing Datastore Fails

When you try to unmount or remove a datastore, the operation fails.

Problem

The operation to unmount or remove a datastore fails if the datastore has any opened files. For these user operations, the vSphere HA agent closes all of the files that it has opened, for example, heartbeat files. If the agent is not reachable by vCenter Server or the agent cannot flush out pending I/Os to close the files, a The HA agent on host '{hostName}' failed to quiesce file activity on datastore '{dsName}' fault is triggered.

Cause

If the datastore to be unmounted or removed is used for heartbeating, vCenter Server excludes it from heartbeating and chooses a new one. However, the agent does not receive the updated heartbeat datastores if it is not reachable, that is, if the host is isolated or in a network partition. In such cases, heartbeat files are not closed and the user operation fails. The operation can also fail if the datastore is not accessible because of storage failures such as all paths down.

Note When you remove a VMFS datastore, the datastore is removed from all the hosts in inventory. So if there are any hosts in a vSphere HA cluster that are unreachable or that cannot access the datastore, the operation fails.

Solution

Ensure that the datastore is accessible and the affected hosts are reachable.

Using Datastore File Browser in the VMware Host Client

Use the datastore file browser to manage the contents of your datastore. You can perform a number of tasks that include uploading files to the datastore, downloading datastore files to your system, moving and copying datastore folders or files, and creating new datastore directories.

Upload Files to a Datastore in the VMware Host Client

Use the datastore file browser to upload files to datastores on your host.

Note Virtual Volumes do not support uploading files directly to the virtual datastores. You must first create a folder on the virtual datastore, and then upload the files into the folder.

In addition to their traditional use as a storage for virtual machine files, datastores can serve to store data or files related to virtual machines. For example, you can upload ISO images of operating systems from a local computer to a datastore on the host. You then use these images to install guest operating systems on the new virtual machines.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Select the datastore that you want to store the file on.
- 4 (Optional) Create a new datastore directory to store the file.
- 5 Select the target folder and click **Upload**

- 6 Locate the item that you want to upload from your local computer and click **Open**.
The file uploads to the datastore that you selected.
- 7 (Optional) Refresh the datastore file browser to see the uploaded file on the list.
- 8 Click **Close** to exit the file browser.

Download Files from a Datastore to Your System in the VMware Host Client

Use the datastore file browser to download files from the datastores available on the host that you are managing to your local system.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Select the target datastore.
- 4 Click the folder that contains the file that you want to download.
The available files in the folder are displayed.
- 5 Click the file that you want to download.
- 6 Click **Download**.
The file is downloaded to your system.
- 7 Click **Close** to exit the file browser.

Delete Files from a Datastore in the VMware Host Client

You can permanently remove files from any datastore if you no longer need them.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Select the target datastore.
- 4 Select the folder that contains the file that you want to delete.
The available files in the folder are displayed.
- 5 Click the file that you want to remove from the datastore, click **Delete**, and click **Delete** again.

- 6 Click **Close** to exit the file browser.

Move Datastore Folders or Files in the VMware Host Client

Use the datastore file browser to move files or folders to a new location, either on the same datastore or on a different datastore.

Note Virtual disk files are moved and copied without format conversion. If you move a virtual disk to a datastore on a type of host that is different from the type of the source host, you might need to convert the virtual disks before you can use them.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Select the target datastore.
- 4 Select the file or folder that you want to move to another location and click **Move**.
- 5 Select your target destination and click **Move**.
- 6 Click **Close** to exit the file browser.

Copy Datastore Folders or Files in the VMware Host Client

Use the datastore file browser to copy folders or files to a new location, either on the same datastore or on a different datastore.

Note Virtual disk files are moved and copied without format conversion. If you move a virtual disk to a datastore on a type of host that is different from the type of the source host, you might need to convert the virtual disks.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Select the target datastore.
- 4 Select the file or folder that you want to move to another location and click **Copy**.
- 5 Select your target destination and click **Copy**.
- 6 Click **Close** to exit the file browser.

Create a New Datastore Directory in the VMware Host Client

You can create new datastore directories if you want to store files in a particular location.

Prerequisites

Required privilege: **Datastore.Browse Datastore**

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Click **File browser**.
- 3 Click **Create directory**.
- 4 Select the target datastore.
- 5 (Optional) Enter a name for the new directory.
- 6 Click **Create directory**.
- 7 Click **Close** to exit the file browser.

Rename a Datastore in the VMware Host Client

You can change the display name of a datastore in the VMware Host Client.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.
- 2 Right-click a datastore in the list and select **Rename** from the drop-down menu.
- 3 Enter a new name for the datastore and click **Save** to apply your changes.
- 4 (Optional) Click **Refresh** to see the new name of the datastore in the list of available datastores.

Delete a VMFS Datastore in the VMware Host Client

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, the datastore and all the files associated to the datastore are removed from the host.

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.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Datastores**.

- 2 Right-click the datastore from the list and select **Delete** from the drop-down menu.
- 3 Click **Confirm** to delete the datastore.

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 in the VMware Host Client

Host hardware acceleration for block storage devices is enabled by default on all hosts. You can use the VMware Host Client advanced settings to disable hardware acceleration.

Changing advanced settings is considered unsupported unless VMware Technical Support instructs you to do so.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Click **Virtual Machines** in the VMware Host Client inventory.
- 2 Right-click the virtual machine in the list and select **Edit Settings** from the drop-down menu.
- 3 On the **VM Options** tab, expand **Advanced**.
- 4 Under **Settings**, select **Disable acceleration**.
- 5 Click **Save**.

Storage Thin Provisioning in the VMware Host Client

With ESXi, you can use two models of thin provisioning, array-level and virtual-disk level thin provisioning.

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, a 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 in the VMware Host Client

To save storage space, you can create thin provisioned virtual disks. The thin provisioned virtual disk starts small and grows as more disk space is required. You can create thin disks only on the datastores that support disk-level thin provisioning.

The following procedure assumes that you are creating a new virtual machine. For more information, see [Creating a Virtual Machine in the VMware Host Client](#).

Procedure

- 1 Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.
The **New Virtual Machine** wizard opens.
- 2 Select a method for adding a new virtual machine on the host and click **Next**.
- 3 Enter a name for your virtual machine.
- 4 Select the virtual machine compatibility from the **Compatibility** drop-down menu.
- 5 Select a guest operating system version from the **Guest OS version** drop-down menu and click **Next**.
- 6 From the list of accessible datastores on the Select storage page of the **New Virtual Machine** wizard, select the destination datastore for the virtual machine configuration files and all of the virtual disks.
- 7 On the **Virtual Hardware** tab, expand **Hard disk**.
- 8 Under **Disk Provisioning**, select the **Thin provisioned** radio button and click **Next**.
- 9 On the Ready to complete page of the **New Virtual Machine** wizard, review the configuration settings for the virtual machine and click **Finish** to save your settings.

View Virtual Machine Storage Resources in the VMware Host Client

You can view how datastore storage space is allocated for your virtual machines in the VMware Host Client.

Resource Consumption shows how much datastore space is occupied by virtual machine files, including configuration files, log files, snapshots, virtual disks, and so on. When the virtual machine is running, the used storage space also includes swap files.

For virtual machines with thin disks, the actual storage usage value might be less than the size of the virtual disk.

Procedure

- 1 Click the virtual machine in the VMware Host Client inventory.
- 2 Review the Resource Consumption information in the lower right area of the virtual machine summary page.

Determine the Disk Format of a Virtual Machine in VMware Host Client

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

Procedure

- 1 Right-click the virtual machine in the VMware Host Client inventory and select **Edit settings**.
- 2 On the **Virtual Hardware** tab, expand **Hard disk**.

The **Type** text box shows the format of your virtual disk.

View Storage Adapters in the VMware Host Client

View the storage adapters that your host uses and related information.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Adapters**.
All storage adapters available to the host are listed under **Adapters**.
- 2 To view details for a specific adapter, select the adapter from the list.

Managing Storage Devices in the VMware Host Client

You can use the VMware Host Client to manage local and networked storage devices that the ESXi host you are managing has access to.

View Storage Devices in the VMware Host Client

View all storage devices available to a host. If you use third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

The Storage Devices view allows you to list the host storage devices, analyze their information, and modify properties.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Devices**.
All storage devices available to the host are listed under **Devices**.
- 2 To view details for a specific device, select the device from the list.

Clear a Device Partition Table in the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can clear the partition table of a disk device that is accessible from the host.

Prerequisites

Verify that the device is not in use by ESXi as boot disk, VMFS datastore, or Virtual SAN.

Procedure

- 1 Click **Storage** in the VMware Host Client and click **Devices**.
- 2 Right-click a device from the list, click **Clear partition table** and click **Yes**.

Clearing the partition table might cause data loss.

Edit Individual Device Partitions in the VMware Host Client

When you log in to an ESXi host with the VMware Host Client, you can remove individual partitions of a device by using the partition editor

Prerequisites

Verify that the device is not in use by ESXi as boot disk, VMFS datastore, or Virtual SAN.

Procedure

- 1 Click **Storage** in the VMware Host Client and click **Devices**.
- 2 Right-click a device from the list and click **Edit partitions**.
- 3 Select a partition and click **Delete partition**.
- 4 (Optional) Click **Reset** to restore the original partitions.
- 5 Click **Save partitions**.
- 6 Confirm that you want to alter the partition.

Monitoring Storage in the VMware Host Client

In the VMware Host Client, you can monitor the storage health of the ESXi host that you are managing. You can also view events and tasks associated with the different datastores, storage adapters, and storage devices on the host that you are managing.

Monitor Datastores in the VMware Host Client

In the VMware Host Client, you can monitor the health of a datastore, as well as events and tasks associated with that datastore.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory.
- 2 Click **Datastores**.
- 3 Click a datastore from the list.
The datastore expands in the VMware Host Client inventory.
- 4 Click **Monitor** under the name of the datastore in the VMware Host Client.
- 5 (Optional) Click **Events** to view events associated with the datastore.
- 6 (Optional) Click **Tasks** to view tasks associated with the datastore.

7 (Optional) Click **Health** to view the datastore health.

Performing Storage Refresh and Rescan Operations in the VMware Host Client

The refresh operation for datastores, storage devices, and storage adapters updates the lists and storage information that the VMware Host Client displays. It updates information such as the datastore capacity. When you perform storage management tasks or make changes in the SAN configuration, you might need to rescan your storage.

Perform Adapter Rescan in the VMware Host Client

When you make changes in your SAN configuration and these changes are isolated to storage accessed through a specific adapter, perform rescan for only this adapter. When you rescan an adapter, you discover any new LUNs that are available on that adapter.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Adapters**.
- 2 Click **Rescan**.

Perform Device Rescan in the VMware Host Client

When you rescan a device, you discover any new VMFS volumes that are available on the device.

Procedure

- 1 Click **Storage** in the VMware Host Client inventory and click **Devices**.
- 2 Click **Rescan**.

Change the Number of Scanned Storage Devices in the VMware Host Client

An ESXi host is limited to accessing 256 SCSI storage devices, but the range of LUN IDs can be from 0 to 1023. ESXi ignores LUN IDs that are 1024 or greater. This limit is controlled by `Disk.MaxLUN`, which has a default value of 1024.

The value of `Disk.MaxLUN` also determines how many LUNs the SCSI scan code attempts to discover by using individual INQUIRY commands if the SCSI target does not support direct discovery by using `REPORT_LUNS`.

You can modify the `Disk.MaxLUN` parameter depending on your needs. For example, if your environment has a smaller number of storage devices with LUN IDs from 0 to 100, you can set the value to 101 to improve device discovery speed on targets that do not support `REPORT_LUNS`. Lowering the value can shorten the rescan time and boot time. However, the time to rescan storage devices might depend on other factors, including the type of storage system and the load on the storage system.

In other cases, you might need to increase the value if your environment uses LUN IDs that are greater than 1023.

Procedure

- 1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
- 2 Scroll down to `Disk.MaxLUN`.
- 3 Right-click `Disk.MaxLUN`, and click **Edit option**.
- 4 Enter a new value and click **Save**.

The SCSI scan code does not scan the LUNs with IDs greater than or equal to the value you enter.

For example, to discover LUN IDs from 0 to 100, set `Disk.MaxLUN` to 101.

Networking in the VMware Host Client

5

When you connect to an ESXi host using the VMware Host Client, you can view and configure vSphere standard switches, port groups, physical NICs, VMkernel NICs, and TCP/IP stacks.

This chapter includes the following topics:

- [Performing Port Group Tasks in the VMware Host Client](#)
- [Managing Virtual Switches in the VMware Host Client](#)
- [Managing Physical Network Adapters in the VMware Host Client](#)
- [Managing VMkernel Network Adapters in the VMware Host Client](#)
- [View TCP/IP Stack Configuration on a Host in the VMware Host Client](#)
- [Change the Configuration of a TCP/IP Stack on a Host in the VMware Host Client](#)
- [Configuring ESXi Firewall in the VMware Host Client](#)
- [Monitoring Networking Events and Tasks in the VMware Host Client](#)

Performing Port Group Tasks in the VMware Host Client

You can use the VMware Host Client to view port group information and to add or modify a virtual machine port group to set up traffic management on a set of virtual machines.

View Port Group Information in the VMware Host Client

In the VMware Host Client, you can view information about port group configuration, network details, virtual switch topology, NIC teaming policy, offload policy, and security policy.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Port groups**.
- 2 Click on an item from the list of available port groups.

Information about network details, virtual switch topology, NIC teaming policy, offload policy, and security policy is displayed.

Add a Virtual Machine Port Group in the VMware Host Client

You can add a port group to a virtual machine in the VMware Host Client. Virtual machine port groups provide networking for virtual machines.

Procedure

- 1 Right-click **Networking** in the VMware Host Client inventory and click **Add port group** from the drop-down menu.
- 2 Enter a name for the new port group.
- 3 Set the VLAN ID to configure VLAN handling in the port group.

The VLAN ID also reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that you entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN.

- 4 Select a virtual switch from the drop-down menu.
- 5 Click **Add port group**.
Your port group is created.
- 6 (Optional) Click **Refresh** to display the new port group in the list.

Edit Port Group Settings in the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can configure various networking settings, such as the port group name, VLAN ID, and virtual switch.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Port groups**.
- 2 Right-click the port group in the list that you want to edit and select **Edit settings**.
- 3 (Optional) Enter a new name for the port group.

Note Changing certain port group names might orphan some virtual machines.

- 4 (Optional) Enter a new value for the VLAN ID.

The VLAN ID reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that you entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN.

- 5 (Optional) Select a virtual switch from the drop-down menu.
- 6 Click **Save port group** to apply your changes.

Remove a Virtual Machine Port Group in the VMware Host Client

You can remove port groups from virtual switches in case you no longer need the associated labeled networks.

Prerequisites

Verify that there are no VMkernel NICs and no powered-on virtual machines connected to the port group that you want to remove.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Port groups**.
- 2 Right-click the port group that you want to remove and select **Remove** from the pop-up menu.
- 3 Click **Confirm** to remove the port group.
- 4 (Optional) Click **Refresh** to verify that you have removed the port group.

Managing Virtual Switches in the VMware Host Client

When you connect to an ESXi host by using the VMware Host Client, you can view, configure and manage vSphere standard switches and uplinks.

View Virtual Switch Information in the VMware Host Client

In the VMware Host Client, you can view information about virtual switches, such as configuration, network details, virtual switch topology, and so on.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
- 2 Click on a switch from the list of available virtual switches.

Information about virtual switch configuration, network details, and virtual switch topology is displayed.

Add a Standard Virtual Switch in the VMware Host Client

In the VMware Host Client, you can add a standard virtual switch to provide network connectivity for the host that you are managing and for the virtual machines on that host, as well as to handle VMkernel traffic. Depending on the type of connection that you want to create, you can create a new vSphere standard switch with a VMkernel adapter, connect an existing physical network adapter to the new switch, or create the switch with a virtual machine port group.

Procedure

- 1 Right-click **Networking** in the VMware Host Client inventory and click **Add standard vSwitch** in the pop-up menu.
- 2 (Optional) Click **Add uplink** to add a new physical uplink to a virtual switch.
- 3 Enter a name for the virtual switch and click **Create virtual switch**.
- 4 Select an uplink for the virtual switch.
- 5 Click **Create virtual switch**.

Remove a Standard Virtual Switch in the VMware Host Client

You can remove a virtual switch if you no longer need it.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
- 2 Right-click the virtual switch that you want to remove from the list and click **Remove**.
- 3 Click **Confirm** to remove the virtual standard switch.

Add a Physical Uplink to a Virtual Switch in the VMware Host Client

You can connect multiple adapters to a single vSphere standard switch to provide NIC teaming. The team can share traffic and provide failover.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
- 2 Click a virtual switch from the list and click **Add uplink**.
- 3 Select a physical NIC from the available options.
- 4 Click **Save**.

Edit Virtual Switch Settings in the VMware Host Client

In the VMware Host Client, you can edit the virtual switch name and the virtual switch uplinks.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
- 2 Right-click the virtual switch that you want to edit and click **Edit Settings**.
- 3 (Optional) Click **Add uplink** to add a new physical uplink to the virtual switch.
- 4 (Optional) Click the **Remove** icon (✕) to remove the old uplink from the virtual switch.
- 5 Click **Save**.

Managing Physical Network Adapters in the VMware Host Client

Assign a physical adapter to a standard switch to provide connectivity to virtual machines and VMkernel adapters on the host that you are managing.

View Physical Network Adapter Information in the VMware Host Client

In the VMware Host Client, you can view various information about physical network adapter (NIC) configuration and settings.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Physical NICs**.
- 2 Click on the network adapter that you want to view information about.

Edit Physical NICs in the VMware Host Client

You can edit physical NIC speed by using the VMware Host Client.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Physical NICs**.
- 2 Select the NIC in the table that you want to edit.
- 3 Click **Edit settings** and select a speed from the drop-down menu.
- 4 Click **Save**.

Managing VMkernel Network Adapters in the VMware Host Client

In the VMware Host Client, you can add and remove VMkernel network adapters (NICs), as well as view and modify the VMkernel NIC settings.

View VMkernel Network Adapter Information in the VMware Host Client

In the VMware Host Client, you can view information about VMkernel network adapters (NICs), such as TCP/IP configuration, network details, virtual switch topology, and so on.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.
- 2 Click on a NIC in the list to display configuration and topology details.

Add a VMkernel Network Adapter in the VMware Host Client

You can add a VMkernel network adapter (NIC) on a vSphere standard switch to provide network connectivity for hosts and to handle the system traffic for vSphere vMotion, IP storage, Fault Tolerance, logging, Virtual SAN, and so on.

Procedure

- 1 Right-click **Networking** in the VMware Host Client inventory and click **Add VMkernel NICs**.
- 2 On the Add new VMkernel interface page, configure the settings for the VMkernel adapter.

Option	Description
Port Group Label	Adding a new VMkernel NIC also adds a new port group. Specify a name for that port group.
VLAN ID	Enter a VLAN ID to determine the VLAN for the network traffic of the VMkernel adapter to use.
IP Version	Select IPv4, IPv6, or both. Note The IPv6 option does not appear on hosts that do not have IPv6 enabled.

- 3 (Optional) Expand the IPv4 settings section to select an option for obtaining IP addresses.

Option	Description
Use DHCP to obtain IP settings	IP settings are obtained automatically. A DHCP server must be present on the network.
Use static IP settings	Enter the IPv4 address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.

- (Optional) Expand the IPv6 settings section to select an option for obtaining IPv6 addresses.

Option	Description
DHCPv6	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Auto Configuration	Use router advertisement to obtain IPv6 addresses.
Static IPv6 Addresses	<ol style="list-style-type: none"> Click Add address to add a new IPv6 address. Enter the IPv6 address and subnet prefix length.

- Select a virtual switch from the drop-down menu.
- Select a TCP/IP stack from the drop-down menu.

After you set a TCP/IP stack for the VMkernel adapter, you cannot change it. If you select the vMotion or the Provisioning TCP/IP stack, you can use only this stack to handle vMotion or for Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are disabled for future vMotion sessions. If you use the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are disabled, and you cannot perform some operations including traffic Provisioning, such as virtual machine cold migration, cloning, and snapshot creation.

- (Optional) Enable vMotion for the default TCP/IP stack on the host.

vMotion enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. It is not possible to use vMotion to perform migrations to selected hosts if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or if no adapters use the vMotion TCP/IP stack.

- Review your setting selections and click **Create**.

Edit VMkernel Network Adapter Settings in the VMware Host Client

You might have to change the supported traffic type for a VMkernel network adapter, or the way IPv4 or IPv6 addresses are obtained.

Procedure

- Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.
- Select the VMkernel adapter that resides on the target standard switch, click **Actions**, and select **Edit settings** from the drop-down menu.
- (Optional) Edit the VLAN ID.
The VLAN ID determines the VLAN that the network traffic of the VMkernel adapter uses.
- (Optional) To edit the IP version, select IPv4, IPv6, or both from the drop-down list.

Note The IPv6 option does not appear on hosts that do not have IPv6 enabled.

- 5 (Optional) Expand the IPv4 settings section to select an option for obtaining IP addresses.

Option	Description
Use DHCP to obtain IP settings	IP settings are obtained automatically. A DHCP server must be present on the network.
Use static IP settings	Enter the IPv4 address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.

- 6 (Optional) Expand the IPv6 settings section to select an option for obtaining IPv6 addresses.

Option	Description
DHCPv6	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Auto Configuration	Use router advertisement to obtain IPv6 addresses.
Static IPv6 Addresses	<ul style="list-style-type: none"> a Click Add address to add a new IPv6 address. b Enter the IPv6 address and subnet prefix length.

- 7 (Optional) Enable or disable vMotion for the default TCP/IP stack on the host.

vMotion enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. It is not possible to use vMotion to perform migrations to selected hosts if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or if no adapters use the vMotion TCP/IP stack.

- 8 Review your setting modifications and click **Save** to apply your changes.

Remove a VMkernel Network Adapter in the VMware Host Client

In the VMware Host Client, you can remove a VMkernel network adapter if you no longer need it.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.
- 2 Right-click the VMkernel adapter that you want to remove and click **Remove**.
- 3 Click **Confirm** to remove the network adapter.

View TCP/IP Stack Configuration on a Host in the VMware Host Client

You can view the DNS and routing configuration of a TCP/IP stack on a host. You can also view the IPv4 and IPv6 routing tables, the congestion control algorithm, and the maximum number of allowed connections.

Procedure

- 1 Click **Networking** in the host inventory and click **TCP/IP stacks**.

- 2 Click a stack from the list.

The configuration settings of the stack you selected are displayed.

Change the Configuration of a TCP/IP Stack on a Host in the VMware Host Client

You can change the DNS and default gateway configuration of a TCP/IP stack on a host. You can also change the congestion control algorithm, the maximum number of connections, and the name of custom TCP/IP stacks.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **TCP/IP stacks**.

- 2 Right-click a stack from the list and select **Edit settings**.

The Edit TCP/IP configuration - Provisioning stack dialog box opens.

- 3 Specify how the host obtains settings for this TCP/IP stack.

- Select the **Use DHCP services from the following adapter** radio button, and select an adapter from which to receive the default settings configuration for the TCP/IP stack.
- Select the **Manually configure the settings for this TCP/IP stack** to change the settings configuration.

Option	Description
Basic configuration	Host name Edit the name of your local host.
	Domain name Edit the domain name.
	Primary DNS server Enter a preferred DNS server IP address.
	Secondary DNS server Type an alternate DNS server IP address.
	Search domains Specify DNS suffixes to use in DNS search when resolving unqualified domain names.
Routing	Edit the IPv4 and IPv6 gateway information.
	Note Removing the default gateway might cause you to lose your connection to the host.
Advanced Settings	Edit the congestion control algorithm and the maximum number of connections.

- 4 Click **Save**.

Configuring ESXi Firewall in the VMware Host Client

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host security profile.

As you open ports on the firewall, consider that unrestricted access to services running on an ESXi host may expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to allow access only from authorized networks.

Note The firewall also allows Internet Control Message Protocol, or ICMP, pings and communication with DHCP and DNS (UDP only) clients.

Manage ESXi Firewall Settings by Using the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can configure incoming and outgoing firewall connections for a service or a management agent.

Note If different services have overlapping port rules, enabling one service might implicitly enable other services. You can specify which IP addresses are allowed to access each service on the host to avoid this problem.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **Firewall rules**.

The VMware Host Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.

- 3 For some services you can manage service details. Right-click a service and select an option from the pop-up menu.
 - Use the **Start**, **Stop**, or **Restart** buttons to change the status of a service temporarily.
 - Change the Startup Policy to configure the service to start and stop with the host, the firewall ports, or manually.

Add Allowed IP Addresses for an ESXi Host by Using the VMware Host Client

By default, the firewall for each service allows access to all IP addresses. To restrict traffic, configure each service to allow traffic only from your management subnet. You can also deselect some services if your environment does not use them.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory and click **Firewall rules**.
- 2 Click a service from the list and click **Edit settings**.
- 3 In the Allowed IP Addresses section, click **Only allow connections from the following networks** and enter the IP addresses of networks that you want to connect to the host.

Separate IP addresses with commas. You can use the following address formats:

- 192.168.0.0/24

- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

4 Click **OK**.

Monitoring Networking Events and Tasks in the VMware Host Client

You can view details about the events and tasks associated with the port groups, virtual switches, physical network adapters, VMkernel network adapters, and TCP/IP stacks on the ESXi host that you are managing.

Monitor Port Groups in the VMware Host Client

In the VMware Host Client, you can monitor port group performance by viewing the events and tasks of the port groups on the host.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **Port groups**.
- 3 Click a port group from the list.
The port group expands in the VMware Host Client inventory.
- 4 Click **Monitor** under the port group name in the VMware Host Client inventory.
- 5 (Optional) Click **Events** to view the events associated with the port group.

Monitor Virtual Switches in the VMware Host Client

In the VMware Host Client, you can monitor virtual switch performance by viewing the events and tasks of the virtual switches on the host.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **Virtual switches**.
- 3 Click a virtual switch from the list.
The virtual switch expands in the VMware Host Client inventory.
- 4 Click **Monitor** under the virtual switch name in the VMware Host Client inventory.
- 5 (Optional) Click **Events** to view the events associated with the virtual switch.

Monitor Physical Network Adapters in the VMware Host Client

In the VMware Host Client, you can monitor physical network adapter (NIC) performance by viewing the events and tasks of the physical NICs on the host.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **Physical NICs**.
- 3 Click a physical network adapter from the list.

The physical network adapter expands in the VMware Host Client inventory.

- 4 Click **Monitor** under the physical network adapter name in the VMware Host Client inventory.
- 5 (Optional) Click **Events** to view the events associated with the physical network adapter.

Monitor VMkernel Network Adapters in the VMware Host Client

In the VMware Host Client, you can monitor VMkernel network adapter performance by viewing the events and tasks of the VMkernel network adapters on the host.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **VMkernel NICs**.
- 3 Click a VMkernel network adapter from the list.

The VMkernel network adapter expands in the VMware Host Client inventory.

- 4 Click **Monitor** under the VMkernel network adapter name in the VMware Host Client inventory.
- 5 (Optional) Click **Events** to view the events associated with the VMkernel network adapter.

Monitor TCP/IP Stacks in the VMware Host Client

In the VMware Host Client, you can monitor TCP/IP stacks performance by viewing the events and tasks of the TCP/IP stacks on the host.

Procedure

- 1 Click **Networking** in the VMware Host Client inventory.
- 2 Click **TCP/IP stacks**.
- 3 Click a TCP/IP stack from the list.

The TCP/IP stack expands in the VMware Host Client inventory.

- 4 Click **Monitor** under the TCP/IP stack name in the VMware Host Client inventory.
- 5 (Optional) Click **Events** to view the events associated with the TCP/IP stack.
- 6 (Optional) Click **Tasks** to view the tasks associated with the TCP/IP stack.