vSphere Single Host Management - VMware Host Client

Update 3

VMware vSphere 7.0

VMware ESXi 7.0

VMware Host Client 1.37.0

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

https://docs.vmware.com/

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

Contents

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

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

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 data center operations.

VMware Host Client Overview

1

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

It is important to know that the VMware Host Client is different from the vSphere Client. You use the vSphere 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

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 32-bit and 64-bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	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 is only used to manage single ESXi hosts. You can use the VMware Host Client to conduct an 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**.

Results

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

You can participate in the Customer Experience Improvement Program (CEIP) to provide anonymous feedback or information to VMware for quality, reliability, and functionality improvments of VMware products and services.

VMware Customer Experience Improvement Program

VMware Tools 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.

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

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 **System**.
2. Click **Advanced settings**.
3. Right-click the appropriate item from the list and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box is displayed.
4. Edit the value and click **Save** to apply your changes.
5. (Optional) Right-click the appropriate item from the list and select **Reset to default** to go back to the original settings of the item.

Create an Initial Welcome Message for the Direct Console User Interface and the VMware Host Client

By using the VMware Host Client, you can create a welcome message that appears on the initial screen of the Direct Console User Interface (DCUI) and on the login window of the VMware Host Client. You can also create a welcome message that appears after a user logs into the VMware Host Client and decide whether to display the welcome message.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

Option	Action
Create a welcome message that appears before you log in to DCUI and VMware Host Client	a Enter **`Annotations.WelcomeMessage`** in the **Search** text box and click the **Search** icon. b Right-click `Annotations.WelcomeMessage` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. c In the **New value** text box, enter the welcome message. To set the default message, leave the **New value** text box blank.
Create a welcome message that appears after you log in to the VMware Host Client	a Enter **`UserVars.HostClientWelcomeMessage`** in the **Search** text box and click the **Search** icon. b Right-click `UserVars.HostClientWelcomeMessage` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. c In the **New value** text box, enter the welcome message. To set the default message, leave the **New value** text box blank.
Enable or disable the appearance of the welcome message after you log in to the VMware Host Client	a Enter **`UserVars.HostClientEnableMOTDNotification`** in the **Search** text box and click the **Search** icon. b Right-click `UserVars.HostClientEnableMOTDNotification` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. c In the **New value** text box, enter the new value. A value of zero (0) disables the appearance of the welcome message. A value of one (1) enables the appearance of the welcome message.

2 Click **Save**.

3 (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure the VMware Host Client User Interface Session Timeout

In VMware Host Client, the User Interface session automatically times out every 15 minutes and then you must log back in to the VMware Host Client.

You can increase the default inactivity timeout by changing an advanced configuration parameter. The default value is 900 seconds.

Procedure

- Configure the User Interface session timeout.

Option	Action
From the VMware Host Client Advanced Settings	a Click **Manage** in the VMware Host Client inventory and click **Advanced Settings** b Enter **`UserVars.HostClientSessionTimeout`** in the **Search** text box and click the **Search** icon. c Right-click `UserVars.HostClientSessionTimeout` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. d In the **New value** text box, enter the timeout setting in seconds. **Note** A value of zero (0) disables the timeout. e Click **Save**. f (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.
From the User Settings drop-down menu	a Click the user name at the top of the VMware Host Client window and select **Settings > Application timeout > .** b To specify the inactivity timeout, select the time. c To disable the inactivity timeout, select `Off`.

Configure the SOAP Session Timeout in the VMware Host Client

In VMware Host Client you can configure the SOAP session timeout.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

2 Enter **`Config.HostAgent.vmacore.soap.sessionTimeout`** in the **Search** text box and click the **Search** icon.

3 Right-click `UserVars.HostClientSessionTimeout` and select **Edit option** from the drop-down menu.

The **Edit option** dialog box opens.

4 In the **New value** text box, enter the timeout setting in seconds.

A value of zero (0) disables the timeout.

5 Click **Save**.

6 (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure the Passwords and Account Lockout Policy in the VMware Host Client

For ESXi hosts, you must use a password with predefined requirements. You can change the required password length, character class requirements, or allow passphrases, all using the `Security.PasswordQualityControl` advanced option. You can also set the number of passwords to remember for each user using the `Security.PasswordHistory` advanced option. The `Security.PasswordMaxDays` advanced option allows you to set up the maximum number of days between password changes.

Note Always perform additional testing after you change the default password settings.

If you attempt to log in with incorrect credentials, the account lockout policy specifies when and for how long the system locks your account.

ESXi Passwords

ESXi enforces password requirements for access.

- By default, when you create a password, you must include a mix of characters from any three of the following four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash.
- By default, the password must contain a length of at least 7 characters and a maximum of 40 characters.
- Passwords must not contain a dictionary word or part of a dictionary word.

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

Example of ESXi Passwords

The following password candidates illustrate potential passwords if the option is set as follows:

```
retry=3 min=disabled,disabled,disabled,7,7
```

With this setting, a user is prompted up to three times (retry=3) for a new password that is not sufficiently strong or if the password was not entered correctly twice. Passwords with one or two character classes and password phrases are not allowed, because the first three items are disabled. Passwords from three and four character classes require 7 characters.

The following password candidates meet the password requirements:

- xQaTEhb!: Contains eight characters from three character classes.
- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet the password requirements:

- Xqat3hi: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of required character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of required character classes is three.

Password Quality Control

You can control the quality of passwords by using the `Security.PasswordQualityControl` advanced option.

`Security.PasswordQualityControl` consists of several settings that follow the pattern:

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

Password Quality Control Settings	Description	Default
`retry=N`	The number of times the user must provide a new password if the password is incorrect or not sufficiently strong.	`retry=3`
`min=N0,N1,N2,N3,N4`	Character class and the passphrase minimum length requirement. ■ `N0` is minimum length of passwords from a single character class. ■ `N1` is minimum length of passwords from two character classes. ■ `N2` is minimum length for a passphrase. ■ `N3` is minimum length for three character classes. ■ `N4` is minimum length for four character classes. You can use `disabled` to disallow a password with the specified number of character classes.	`min=disabled,disabled,disabled,7,7`
`max=N`	The maximum allowed password length.	`max=40`

Password Quality Control Settings	Description	Default
`passphrase=N`	The number of words required for a passphrase. To make sure that the `passphrase` is recognized, do not set `N2` from the `min` setting to `disabled`.	`passphrase=3`
`similar=permit|deny`	Indicates whether a password is allowed to be similar to the old password. To use this setting, make sure that you set the `Security.PasswordHistory` option to a non-zero value.	`similar=deny`

ESXi Passphrase

Instead of a password, you can use a passphrase. Passphrases are disabled by default. You can change the default setting by using the `Security.PasswordQualityControl` advanced option.

For example, you can change the option to the following.

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows passphrases of at least 16 characters. The passphrase must consist of at least 3 words, separated by spaces.

Example Password History and Rotation Policy

To remember a history of 5 passwords, set the `Security.PasswordHistory` option to 5.

To enforce a 90 day password rotation policy, set the `Security.PasswordMaxDays` option to 90.

ESXi Account Lockout Policy

Users are locked out after a preset number of consecutive failed attempts. By default, users are locked out after 5 consecutive failed attempts in 3 minutes and a locked account is unlocked automatically after 15 minutes by default. You can change the maximum allowed failed attempts and the period of time in which the user account is locked out by using the `Security.AccountLockFailures` and `Security.AccountUnlockTime` advanced options.

To configure the administrator passwords and account lockout behaviour, perform the following steps.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

Option	Action
Configure the required password length, character class requirement, or allow passphrases	a Enter **`Security.PasswordQualityControl`** in the **Search** text box and click the **Search** icon. b Right-click `Security.PasswordQualityControl` and select **Edit option** from the drop-down menu.
Configure the number of passwords to remember for each user	a Enter **`Security.PasswordHistory`** in the **Search** text box and click the **Search** icon. b Right-click `Security.PasswordHistory` and select **Edit option** from the drop-down menu. **Note** Zero deactivates password history.
Configure the maximum number of days between password changes	a Enter **`Security.PasswordMaxDays`** in the **Search** text box and click the **Search** icon. b Right-click `Security.PasswordMaxDays` and select **Edit option** from the drop-down menu.
Configure the number of failed login attempts allowed before lockout	a Enter **`Security.AccountLockFailures`** in the **Search** text box and click the **Search** icon. b Right-click `Security.AccountLockFailures` and select **Edit option** from the drop-down menu. **Note** Zero (0) deactivates account locking.
Configure the period of time in which the user's account is locked out	a Enter **`Security.AccountUnlockTime`** in the **Search** text box and click the **Search** icon. b Right-click `Security.AccountUnlockTime` and select **Edit option** from the drop-down menu.

The **Edit option** dialog box opens.

2 In the **New value** text box, enter the new setting.

3 Click **Save**.

4 (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Syslog in the VMware Host Client

To configure the syslog service, you can use the VMware Host Client.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

2 In the **Search** text box, enter the name of the setting that you want to change and click the **Search** icon.

Option	Description
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and the port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `protocol://hostName1:port` where `protocol` can be udp, tcp, or ssl. You can use only port 514 for UDP. The ssl protocol uses TLS 1.2. For example: `ssl://hostName1:1514`. The value of `port` can be any decimal number between 1 and 65535. While no hard limit to the number of remote hosts to receive syslog messages exists, it is recommended to keep the number of remote hosts to five or less.
Syslog.global.logCheckSSLCerts	Enforce checking of the SSL certificates when you log in to a remote host.
Syslog.global.defaultRotate	Maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. Specify the directory as [*datastorename*] *path_to_file*, where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.

3 Right-click the setting name and select **Edit option** from the drop-down menu.

The **Edit option** dialog box opens.

4 To perform the SSL certificates check when you log in to a remote host, click **True** from the **New value**.

5 Click **Save**.

6 (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Advanced TLS/SSL Key Options

You can configure the security protocols and cryptographic algorithms that are used to encrypt communications with the ESXi host.

The Transport Layer Security (TLS) key secures communication with the host using the TLS protocol. Upon first boot, the ESXi host generates the TLS key as a 2048-bit RSA key. Currently, ESXi does not implement automatic generation of ECDSA keys for TLS. The TLS private key is not intended to be serviced by the administrator.

The SSH key secures communication with the ESXi host using the SSH protocol. Upon first boot, the system generates the SSH key as a 2048-bit RSA key. The SSH server is deactivated by default. SSH access is intended primarily for troubleshooting purposes. The SSH key is not intended to be serviced by the administrator. Logging in through SSH requires administrative privileges equivalent to full host control. To enable SSH access, see Enable the Secure Shell (SSH) in the VMware Host Client.

You can configure the following ESXi host security key settings.

Key	Default	Description
`UserVars.ESXiVPsAllowedCiphers`	**`! aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES`**	The default cipher control string.
`UserVars.ESXiVPsDisabledProtocols`	**`sslv3,tlsv1,tlsv1.1`**	By default enables TLS v1.0, v1.1, and v1.2 protocols. SSL v3.0 is disabled. If you do not specify a protocol, all protocols are enabled.
`Config.HostAgent.ssl.keyStore.allowAny`	**`False`**	You can add any certificate to the ESXi CA trust store.
`Config.HostAgent.ssl.keyStore.allowSelfSigned`	**`False`**	You can add non-CA self-signed certificates to the ESXi CA trust store, that is, certificates that do not have the CA bit set.
`Config.HostAgent.ssl.keyStore.discardLeaf`	**`True`**	Discards leaf certificates added to the ESXi CA trust store.

To configure the ESXi security key settings:

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter the security key in the **Search** text box and click the **Search** icon.
3. Right-click the security key and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box opens.
4. In the **New value** field entre the new value and click **Save**.
5. (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Userworld Memory Zeroing

With VMware Host Client, you can use the advanced option `Mem.MemEagerZero` to determine how pages are zeroed out for virtual machines and user space applications.

To zero all pages when they allocated to virtual machines and user space applications, set the default value of `Mem.MemEagerZero` to zero (0). If the memory is not reused, this default setting prevents exposing the information from a virtual machine to other clients while preserving the previous content in memory.

When you set `Mem.MemEagerZero` to 1, pages are zeroed when a user space application exits. For virtual machines, such pages are zeroed if:

- The virtual machine is powered off.
- The virtual machine pages are migrated.
- The ESXi host reclaims virtual machines memory.

Note For virtual machines, you can obtain this behaviour by setting the `sched.mem.eagerZero` advanced option to **`TRUE`**.

For information about setting the advanced virtual machine options, see the *vSphere Resource Management* documentation.

To configure the userworld memory zeroing, perform the following steps.

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter **`Mem.MemEagerZero`** in the **Search** text box and click the **Search** icon.
3. Right-click `Mem.MemEagerZero` and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box opens.
4. In the **New value** text box, enter the new value.

   The default value is zero (0).
5. Click **Save**.
6. (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Change Autostart Configuration in the VMware Host Client

Configure autostart options for the ESXi host to set up when the host starts and stops.

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **System**.
2. Click **Autostart**.
3. Click **Edit settings**.

4 Select **Yes** to enable changing the autostart configuration.

Option	Description
Start delay	Configure the start time of the host.
Stop delay	Configure the stop time of the host.
Stop action	Select the **System default**, **Power off**, **Suspend**, or **Shut down** option.
Wait for heartbeat	Select **Yes** to enable the **Wait for heartbeat** option.

5 Click **Save**.

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

By using the VMware Host Client, you can configure the time settings of a host manually or can synchronize the time and date of the host with an NTP or a PTP server. NTP provides millisecond timing accuracy and PTP maintains microsecond timing accuracy.

The NTP service on the host periodically takes the time and date from the NTP server. You can use the **Start**, **Stop**, or **Restart** buttons to change the status of the NTP service on the host at any time regardless of the selected startup policy for the NTP service.

PTP provisions precise time synchronization for the virtual machines within a network. To change the PTP service on the host at any time, you can use the **Start**, **Stop**, or **Restart** buttons. Starting or stopping the PTP service automatically enables or disables PTP. To apply the change when you enable or disable PTP manually, start or stop the PTP service.

For more information about services, see Manage Services in the VMware Host Client.

Note The NTP and PTP services cannot run simultaneously.

Procedure

1 In the VMware Host Client navigator pane, click **Manage**.

2 On the **System** tab, click **Time & date**.

3 Set the time and date for the host.

Option	Action
Manually configure the date and time on this host	a Click **Edit NTP Settings**. The **Edit NTP Settings** dialog box appears. b Set the time and date for the host manually. c Click **Save**.
Use Network Time Protocol (Enable NTP client)	a Click **Edit NTP Settings**. The **Edit NTP Settings** dialog box appears. b Select the **Use Network Time Protocol** radio button. c In the **NTP Servers** text box, enter the IP addresses or host names of the NTP servers that you want to use. d From the **NTP Service Startup Policy** drop-down menu, select an option for starting and stopping the NTP service on the host. ■ **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 and shuts down. ■ **Start and stop manually**. Enables manual starting and stopping of the NTP service. If you select the **Start and stop manually** policy, the status of the NTP service changes only when you use the UI controls. e Click **Save**.
Use Precision Time Protocol (Enable PTP client)	a Click **Edit PTP Settings**. b Select the **Enable** check box. c From the **Network interface** drop-down menu, select a network interface. The IPv4 and Subnet mask appear. d Click **Save**.

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**.

Change the Hardware Label in the VMware Host Client

In the VMware Host Client, you can change the hardware label of all available PCI passthrough devices on a virtual machine. You use hardware labels to restrict the virtual machine placement to specific hardware instances. You can add all available devices with the same hardware label or with a blank hardware label to a virtual machine.

Procedure

1. In the VMware Host Client navigator pane, click **Manage**.

2 On the **Hardware** tab, click **PCI Devices**.

3 Select an available device from the list and click **Hardware label**.

   The toggle passthrough must be active for the selected device.

   The **Edit Hardware Label** dialog box appears.

4 Edit the hardware label and click **Save** to apply the changes.

Results

The new hardware label appears in the hardware label column.

Licensing for ESXi Hosts

ESXi hosts are licensed with vSphere licenses. Each vSphere license has a certain capacity that you can use to license multiple physical CPUs on ESXi hosts.

Starting with vSphere 7.0, one CPU license covers one CPU with up to 32 cores. If a CPU has more than 32 cores, you need additional CPU licenses.

Number of CPUs	Cores per CPU	Number of CPU Licenses
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

When you assign a vSphere license to a host, the amount of capacity consumed is determined by the number of physical CPUs on the host and the number of cores in each physical CPU. 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 capacity to license all physical CPUs on the host.
- 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.

If you use the licensing model with up to 32 cores, you can assign a vSphere license for 10 32-core CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts with 32 cores per CPU
- Five 1-CPU hosts with 64 cores per CPU
- Two 2-CPU hosts with 48 cores per CPU and two 1-CPU hosts with 20 cores per CPU

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

After you install ESXi, it operates in evaluation mode for up to 60 consecutive days. An evaluation mode license provides all features of the highest vSphere product edition.

After you assign a license to an ESXi host, at any time before the evaluation period expires, you can set the host back to evaluation mode to explore the entire set of features available for the remaining evaluation period.

For example, if you use an ESXi host in evaluation mode for 20 days, then assign a vSphere Standard license to the host, and 5 days later set the host back to evaluation mode, you can explore the entire set of features available for the host for the remaining 35 days of the evaluation period.

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 before the license expiration.

Note When there are expiring licenses, a notification appears 90 days before the license expiration.

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 major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade an ESXi host from 5.x to 6.x, you must license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license use 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

- Click **Manage** in the VMware Host Client inventory and click **Licensing**.

  You can view the license key, the expiration date, and all 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.

Note If you use vCenter Server to manage your ESXi host, you can only change your licenses from the vSphere Client.

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 Customer Connect, you must remove the old licenses.

For example, suppose that you have upgraded a vSphere license from 6.5 to 6.7 in Customer Connect. You assign the license to ESXi 6.7 hosts. After assigning the new vSphere 6.7 licenses, you must remove the old vSphere 6.5 license from the inventory.

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **Licensing**.
2. Click **Remove license**, and click **OK**.

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

You can add ESXi hosts to an Active Directory domain by using vSphere Authentication Proxy instead of adding the hosts explicitly to the Active Directory domain.

You only have to set up the host so it knows about the domain name of the Active Directory server and about the IP address of vSphere Authentication Proxy. When vSphere Authentication Proxy is enabled, it automatically adds hosts that are being provisioned with Auto Deploy to the Active Directory domain. You can also use vSphere Authentication Proxy with hosts that are not provisioned by using Auto Deploy.

See #unique_37 for information about TCP ports used by vSphere Authentication Proxy.

See *vSphere Security* for details on setting up vSphere Authentication Proxy.

Auto Deploy

If you are provisioning hosts with Auto Deploy, you can set up a reference host that points to Authentication Proxy. You then set up a rule that applies the reference host's profile to any ESXi host that is provisioned with Auto Deploy. vSphere Authentication Proxy stores the IP addresses of all hosts that Auto Deploy provisions using PXE in its access control list. When the host boots, it contacts vSphere Authentication Proxy, and vSphere Authentication Proxy joins those hosts, which are already in its access control list, to the Active Directory domain.

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 if you follow the instructions for using custom certificates with Auto Deploy.

Other ESXi Hosts

You can set up other hosts to use vSphere Authentication Proxy if you want to make it possible for the host to join the domain without using Active Directory credentials. That means you do not need to transmit Active Directory credentials to the host, and you do not save Active Directory credentials in the host profile.

In that case, you add the host's IP address to the vSphere Authentication Proxy access control list, and vSphere Authentication Proxy authorizes the host based on its IP address by default. You can enable client authentication to have vSphere Authentication Proxy check the host's certificate.

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

You can use the certificate information 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:

Option	Description
Generate FQDN signing request	■ Click **Generate FQDN signing request**, click the **Copy to clipboard** button, and click **Close**. ■ To generate the signed certificate, pass the certificate signing request to the certificate authority (CA). ■ In the **Certificate** text box, paste the generated signed certificate in PEM format and click **Import**.
Generate IP signing request	■ Click **Generate IP signing request**, click the **Copy to clipboard** button, and click **Close**. ■ To generate the signed certificate, pass the certificate signing request to the CA. ■ In the **Certificate** text box, paste the generated signed certificate in PEM format and click **Import**.

You do not have to import the certificate immediately. To make sure that you can use the signed certificate, do not restart the host between generating the certificate signing request and importing the certificate.

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

An FQDN request has the fully qualified host name 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.

Managing Users with the VMware Host Client

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

Users and roles control who has access to the ESXi host components and what actions each user can perform.

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

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

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

Add an ESXi User in the VMware Host Client

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

Prerequisites

For information about password requirements, see Configure the Passwords and Account Lockout Policy in the VMware Host Client or the *vSphere Security* documentation.

Procedure

1 Log in to ESXi with the VMware Host Client.

You cannot create ESXi users with the vSphere Client. You must directly log in to the host with the VMware Host Client to create ESXi users.

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

3 Click **Users**.

4 Click **Add user**.

5 Enter a user name, and a password.

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

- Do not include any spaces in the user name.
- Do not include any non-ASCII characters in the user name.
- Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, an error message indicates password requirements.

6 Click **Add**.

Update an ESXi User in the VMware Host Client

You can change the description and password for an ESXi user in the VMware Host Client.

Procedure

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

2 Click **Users**.

3 Select a user from the list and click **Edit user**.

4 Update the user details and click **Save**.

Remove a Local ESXi User from a Host in the VMware Host Client

You can remove a local ESXi user from the host.

Caution Do not remove the root user.

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

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

Procedure

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

2 Click **Users**.

3 Select the user that you want to remove from the list, click **Remove user**, and click **Yes**.

   Do not remove the root user for any reason.

Managing ESXi Roles in the VMware Host Client

ESXi grants access to objects only to users who are assigned permissions for the object. When you assign a user permission for the object, you do so by pairing the user with a role. A role is a predefined set of privileges. For more information about privileges, see the *vSphere Security* documentation.

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

You can create custom roles by using the role-editing functions in the VMware Host Client to create privilege sets that match your user needs. Also, the roles you create directly on a host are not accessible in vCenter Server. You can work with these roles only if you log in to the host directly from the VMware Host Client.

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

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

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

Add a Role in the VMware Host Client

You can create roles to suit the access control needs of your environment.

Prerequisites

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

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
2. Click **Roles**.
3. Click **Add role**.
4. Enter a name for the new role.
5. Select privileges from the list to associate with the new role and click **Add**.

Update a Role in the VMware Host Client

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

Prerequisites

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

Procedure

1. Click **Manage** in the VMware Host Client inventory and click **Security & Users**.
2. Click **Roles**.
3. Select a role from the list and click **Edit role**.
4. Update the role details and click **Save**.

Remove a Role in the VMware Host Client

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

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

Prerequisites

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

Procedure

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

3 Select the name of the role that you want to remove from the list.

4 Click **Remove role**, select **Remove only if unused**, and click **Yes**.

Managing Hosts in vCenter Server

To monitor all hosts in your virtual environment from one place and to simplify host configuration, connect the hosts 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.

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 or a datastore path to either a VIB or the `metadata.zip` file in an ESXi offline bundle package.

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

If you provide an offline bundle, you update the entire ESXi host to the version described by the `metadata.zip` file in the bundle. Make sure that the entire offline bundle is available through the URL or is uploaded to the datastore.

Procedure

- To update your environment to the latest version, perform the following tasks:

Task	Steps
Upload a VIB to a datastore	a Click **Storage** from the VMware Host Client environment. b Select a datastore from the list and click **Datastore browser**. c To store the VIB, select a directory and click **Upload**. d Browse to and double-click the file.
Upload an offline bundle to a datastore	a Download the ESXi offline bundle package. b Upload the ESXi offline bundle package to the ESXi host. You can either upload the offline bundle package by using the **Datastore browser** or by using SCP or WinSCP. c Extract the contents of the offline bundle on the ESXi host. For example, log in to the host by using SSH. d Navigate to the directory where you uploaded the offline bundle. e Extract the contents by using the `unzip` command.
Update your environment	a Click **Manage** in the VMware Host Client and click **Packages**. b Click **Install update** and enter the URL or the datastore path to a VIB or a `metadata.zip` file in an offline bundle. c Click **Update**. **Caution** If you update an ESXi host managed by vSphere Lifecycle Manager, the host might become non-compliant. d Click **Refresh** to make sure that the update is successful.

Unable to Connect from the VMware Host Client to an ESXi Host After Upgrading to ESXi 6.0 or Later

After you upgrade your host from ESXi 5.5 to ESXi 6.0 or later, your browser console might display an error message when you attempt to access your ESXi host by using the VMware Host Client, and your connection might fail.

Problem

After you upgrade your ESXi host from 5.5 to 6.0 or later, attempting to navigate to **`http://host-name/ui`** or **`http://host-IP-address/ui`** might result in the following error:

```
503 Service Unavailable (Failed to connect to endpoint:
[N7Vmacore4Http16LocalServiceSpecE:0xffa014e8] _serverNamespace = /ui _isRedirect = false
_port = 8308)
```

Cause

A change to `/etc/vmware/rhttpproxy/endpoints.conf` remains after an upgrade and causes the `/ui` endpoint to override the VMware Host Client.

When the `/ticket` is missing from the `endpoint.conf` file on your 6.0 or later ESXi host, your in-browser virtual machine console displays a `Failed to connect` error message but the VMware Remote Console continues to work.

Solution

1 Log in to your ESXi host either by using SSH or ESXi Shell.

   If you use SSH, you might need to enable SSH first. You can enable SSH by using DCUI.

2 Back up the `endpoints.conf` file.

```
cp
        /etc/vmware/rhttpproxy/endpoints.conf /tmp
```

3 Open the `/etc/vmware/rhttpproxy/endpoints.conf` file in an editor and remove the following line.

```
 /ui local 8308 redirect
        allow
```

4 Restart the reverse Web proxy .

```

        /etc/init.d/rhttpproxy restart
```

5 Try to access the VMware Host Client at **http://host-name/ui** or **http://host-IP-address/ui**.

Switch to the vSphere 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 vSAN cluster, you might lose access to the vSAN data on the host.

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

Using the ESXi Shell

The ESXi Shell is disabled by default on ESXi hosts. You can enable local and remote access to the shell if necessary.

To reduce the risk of unauthorized access, enable the ESXi Shell for troubleshooting only.

The ESXi Shell is independent of lockdown mode. Even if the host is running in lockdown mode, you can still log in to the ESXi Shell if it is enabled.

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.

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 run system commands (such as `vmware -v`) by using the ESXi Shell.

Note Do not enable the ESXi Shell unless 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.

Create a Timeout for ESXi Shell Availability in the VMware Host Client

The ESXi Shell is disabled by default. To increase security when you enable the shell, you can set an availability timeout for the ESXi Shell.

The availability timeout defines how long both local and remote shell logins are allowed before the ability to log in through the shell is disabled. When the availability timeout expires, any existing shell sessions remains, but new shell sessions are not allowed.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

2 Enter **`UserVars.ESXiShellTimeOut`** in the **Search** text box and click the **Search** icon.

3 Right-click `UserVars.ESXiShellTimeOut` and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box opens.

4 In the **New value** text box, enter the timeout setting.

   A value of zero (0) disables the timeout.

5 Click **Save**.

   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.

6 (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Create a Timeout for Idle ESXi Shell Sessions in the VMware Host Client

If you enable the ESXi Shell on a host, but forget to log out of the session, the idle session remains connected indefinitely. The open connection increases the potential for someone to gain privileged access to the ESXi host. Prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before you are logged out of an idle interactive session.

Procedure

1 Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

2 Enter **`UserVars.ESXiShellInteractiveTimeOut`** in the **Search** text box and click the **Search** icon.

3 Right-click `UserVars.ESXiShellInteractiveTimeOut` and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box opens.

4. In the **New value** text box, enter the timeout setting.

   A value of zero (0) disables the timeout.

5. Click **Save**.

   The timeout takes effect only for newly logged in sessions.

6. (Optional) To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Results

If the session is idle, users are logged out after the timeout period elapses.

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**.

Results

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

Managing Permissions in the VMware Host Client

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

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

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

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

Many tasks require permissions on more than one object. The following rules can help you determine which roles to assign to users to allow particular tasks:

- Any task that consumes hard disk space, such as creating a virtual disk or taking a snapshot, requires the **Datastore.Allocate Space** privilege on the target datastore and the privilege to perform the operation itself.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege.

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

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

Permission Validation

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

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

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

Assign Permissions to a User for an ESXi Host in the VMware Host Client

To perform particular activities on an ESXi host, a user must have permissions that are associated with a particular role. In the VMware Host Client, you can assign roles to users and give the users the permissions necessary to perform various tasks on the host.

Procedure

1. Right-click **Host** in the VMware Host Client inventory and click **Permissions**.
2. Click **Add user**.
3. Click the arrow next to the **Select a user** text box and select the user that you want to assign a role to.
4. Click the arrow next to the **Select a role** text box and select a role from the list.
5. (Optional) Select **Propagate to all children** or **Add as group**.

   If you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and other objects in the vCenter Server instance.
6. Click **Add** and click **Close**.

Remove Permissions for a User in the VMware Host Client

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

Procedure

1. Right-click **Host** in the VMware Host Client inventory and click **Permissions**.
2. Select a user from the list and click **Remove user**.
3. Click **Close**.

Assign a User Permissions for a Virtual Machine in the VMware Host Client

Assign a role to a particular user to give that user permissions to perform specific tasks on a virtual machine.

Procedure

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Right-click a virtual machine from the list and select **Permissions**.
3. Click **Add user**.

4. Click the arrow next to the **Select a user** text box and select the user that you want to assign a role for.
5. Click the arrow next to the **Select a role** text box and select a role from the list.
6. (Optional) Select **Propagate to all children**.

   If you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and similar objects in the vCenter Server instance.
7. Click **Add** and click **Close**.

Remove Permissions for a Virtual Machine in the VMware Host Client

To make a user unable to perform tasks on a particular virtual machine, remove the permissions of the user for that virtual machine.

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

Procedure

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Right-click a virtual machine from the list and select **Permissions**.
3. Select a user from the list and click **Remove user**.
4. Click **Close**.

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 box 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.

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 and later, 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 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, the DCUI service is stopped. If the connection to vCenter Server is lost and the vSphere 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 theVMware 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

With vSphere 6.0 and later, 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.

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 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 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 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.

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

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.

Procedure

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.
- **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. (Optional) Select the **Enable Windows Virtualization Based Security** check box to enable VBS on the virtual machine.

   The **Enable Windows Virtualization Based Security** check box only appears if you chose a Windows OS version that supports VBS and if the virtual machine's compatibility is ESXi 6.7 and later.

   Important Enabling VBS automatically exposes hardware assisted virtualization and IOMMU to the guest OS and makes EFI and secure boot available.

6. 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. On the Select storage page, choose the type of storage for the virtual machine.
   - Click the **Standard** button to save all the virtual machine disks and configuration files on a standard datastore.
   - Click the **Persistent Memory** button to save the virtual machine hard disks on the host-local PMem datastore.
2. Choose a datastore from the list.

   Important The configuration files cannot be stored on a PMem datastore. If you choose to use PMem, you must select a regular datastore for the configuration files of the virtual machine.

3 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 (Optional) On the Customize settings page, click **Virtual Hardware** and add a new virtual hardware device.

- Click the **Add hard disk** icon to add a new virtual hard disk.

  Note You can add a standard or a persistent memory hard disk to the virtual machine. The persistent memory hard disk is stored on the host-local PMem datastore.

- Click the **Add network adapter** icon to add a NIC to the virtual machine.
- Click the **Add other device** icon to choose other type of device to add to the virtual machine.

  Note If the virtual machine uses PMem storage, the hard disks that are stored on a PMem datastore and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

2 (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: ■ 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.
PCI device	You can configure PCI devices on an ESXi host to make them available for passthrough. You can also change the hardware label to restrict the virtual machine placement to specific hardware instances.
Dynamic PCI device	PCI passthrough devices are automatically grouped by their vendor and model name. You can configure the desired devices by the vendor and model name instead of selecting a physical PCI device by the hardware address. You can add all available devices with the same hardware label or with a blank hardware label to a virtual machine. When you power on a virtual machine, specific physical PCI passthrough devices with matching vendor and model names attach to the virtual machine.
Security devices	You can configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines and provide additional security to your workloads. You can enable or disable vSGX when you create a virtual machine or edit an existing virtual machine.

3 To remove a device, click the delete icon (⊗) next to the device.

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

4 (Optional) Click the **VM Options** button to customize virtual machine options.

5 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 Click **Finish** to complete the creation task and close the wizard.

Results

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 application 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 action 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.

Procedure

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. Mozilla Firefox has a 4 GB 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. On the Select storage page, choose the type of storage for the virtual machine.

   - Click the **Standard** button to save all the virtual machine disks and configuration files on a standard datastore.
   - Click the **Persistent Memory** button to save the virtual machine hard disks on the host-local PMem datastore.

2. Choose a datastore from the list.

   Important The configuration files cannot be stored on a PMem datastore. If you choose to use PMem, you must select a regular datastore for the configuration files of the virtual machine.

3. 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.

Results

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

Registering Existing Virtual Machines in the VMware Host Client

If you unregister a virtual machine from a host but you do not delete the virtual machine from the datastore, you can re-register the virtual machine by using the VMware Host Client. Re-registering a virtual machine makes it appear in the inventory once again.

Procedure

1. Register an Existing Virtual Machine in the VMware Host Client

   The **New virtual machine** wizard allows you to select one or more virtual machines that you would like to register.

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

The **New virtual machine** wizard allows you to select one or more virtual machines that you would like to register.

Use the datastore browser to select either a datastore, a directory, or a `.vmx` file to add to the list of virtual machines that you register. Selecting a datastore or directory searches for all `.vmx` files in that location. You can browse more than once to append virtual machines to the list.

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.

The **New virtual machine** wizard allows you to select one or more virtual machines that you would like to register. By selecting a datastore or a directory, you choose to register all virtual machines on that datastore or in that directory.

Procedure

1. Click **Select one or more virtual machines, a datastore, or a directory**, locate the virtual machine or virtual machines that you would like to register, and click **Select**.
2. (Optional) To remove a virtual machine from the list, select the name of the file and click **Remove selected**.
3. (Optional) To clear your selection and start again, click **Remove all**.
4. 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

VMware Remote Console 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*. 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. VMRC can also modify virtual machine settings such as RAM, CPU cores, and disks. 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.

For a full set of console features, download and install VMRC.

Install the VMware Remote Console Application in the VMware Host Client

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

Procedure

1 Click **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 the **Console** toolbar icon and select the **Download VMRC** option.

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 standalone application for the selected virtual machine.

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 the **Console** tool bar icon and select whether to open the console in a pop-up window, new window, or a new tab.

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 or 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

◆ Click **Virtual Machines** in the VMware Host Client inventory, select a virtual machine, and select your task.

  - To shut down a virtual machine, right-click the virtual machine and select **Guest OS > Shut down**.
  - To restart a virtual machine, right-click the virtual machine and select **Guest OS > 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.

   If you choose a Windows OS version that supports VBS and if the virtual machine's compatibility is ESXi 6.7 and later, the VBS row appears on the **VM Options** tab.

4 (Optional) Click the **Enable Virtualization Based Security** to enable VBS.

   Important Enabling VBS requires that you use EFI to boot the virtual machine. Changing the firmware might make the guest OS unbootable.

5 Click **Save** to apply your changes.

Results

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 set of services and modules that enable several features in VMware products for better management of guests operating systems and seamless user interactions with them.

VMware Tools has the ability to:

- Pass messages from the host operating system to the guest operating system.
- Customize guest operating systems as a part of the vCenter Server and other VMware products.
- Run scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.
- Synchronize the time in the guest operating system with the time on the host operating system

VMware Tools Lifecycle Management provides a simplified and scalable approach for installation and upgrade of VMware Tools. It includes a number of feature enhancements, driver-related enhancements, and support for new guest operating systems.

You must run the latest version of VMware Tools or use open-vm-tools distributed with the Linux OS distribution. Although a guest operating system can run without VMware Tools, you must always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates.

You can configure your virtual machine to automatically check 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 Guide*

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 *VMware Tools User 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 the *VMware Tools User 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 newer versions of VMware Tools and install them.

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.

For vSphere virtual machines, when the installed version of VMware Tools is outdated, the status bar displays the message:

```
A newer version of Tools is available for this VM
```

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, in case of 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. The procedure is mentioned below.

Note Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver allows 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 vSphere Lifecycle Manager to perform an orchestrated upgrade of virtual machines at the folder or data center 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 7.0 Update 3 and later	This virtual machine (hardware version 19) is compatible with ESXi 7.0 Update 3 and later.
ESXi 7.0 Update 2 and later	This virtual machine (hardware version 19) is compatible with ESXi 7.0 Update 2 and later.

Table 3-1. Virtual Machine Compatibility Options (continued)

Compatibility	Description
ESXi 7.0 Update 1 and later	This virtual machine (hardware version 18) is compatible with ESXi 7.0 Update 1 and ESXi 7.0 Update 2.
ESXi 7.0 and later	This virtual machine (hardware version 17) is compatible with ESXi 7.0, ESXi 7.0 Update 1, and ESXi 7.0 Update 2.
ESXi 6.7 Update 2 and later	This virtual machine (hardware version 15) is compatible with ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, and ESXi 7.0 Update 2.
ESXi 6.7 and later	This virtual machine (hardware version 14) is compatible with ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, and ESXi 7.0 Update 2.
ESXi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, and ESXi 7.0 Update 2.
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0, ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, and ESXi 7.0 Update 2.

For more information, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility.

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.
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.
Put Guest on Standby	Puts the guest operating system on standby. This option stops all processes, but all virtual devices remain connected to the virtual machine.
System 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. In the Configuration Parameters row, click **Edit Configuration**.

   The **Configuration Parameters** dialog box opens.
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 **OK** to save your changes and exit the **Configuration Parameters** dialog box.
8. 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 applications to run. The CPU 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 applications. Cores can independently run applications or threads. One or more cores can exist on a single CPU.

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 is 768. The number of virtual CPUs depends on 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 or two times that number if hyperthreading is enabled.
- If a running virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a running virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.
- The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this functionality 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 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 with ESXi 7.0 Update 1 and later compatibility to have up to 768 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.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

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

Change the Number of Virtual CPUs in the VMware Host Client

A virtual machine with ESXi 7.0 Update 1 and later compatibility can have up to 768 virtual CPUs. You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hot add 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 the running virtual machine. You can add only multiples of the number of cores per socket.

If a virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

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

Prerequisites

- If CPU hot add is not enabled, 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 4 MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96 MB of RAM or they cannot power on.

Maximum memory size for virtual machines that use BIOS firmware is 24560 GB. You must use EFI firmware for virtual machines with memory size greater than 6128 GB.

Maximum memory size for a virtual machine depends on the physical memory of the ESXi host and the virtual machine compatibility settings.

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 physical memory of the ESXi host 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 4 MB.

Table 3-2. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 7.0 Update 2	ESXi 7.0 Update 2 and later	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 and later	24560 GB
ESXi 7.0	ESXi 7.0 and later	6128 GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 and later	6128 GB
ESXi 6.7	ESXi 6.7 and later	6128 GB
ESXi 6.5	ESXi 6.5 and later	6128 GB
ESXi 6.0	ESXi 6.0 and later	4080 GB
ESXi 5.5	ESXi 5.5 and later	1011 GB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESXi 5.5 and later compatibility running on ESXi 6.0 is restricted to 1011 GB.

Prerequisites

- Power off the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Change Memory** privilege on the virtual machine.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory** and change the memory configuration.
   a. In the **Memory** text box, enter the amount of RAM to assign to the virtual machine.
   b. Select whether the memory is specified in MB, GB or TB.
3. Click **OK**.

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 *vSphere Resource Management* 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 enable **Memory Hot Plug**.

4 Click **Save**.

Add an NVDIMM device to a VM in the VMware Host Client

Add a virtual NVDIMM device to a virtual machine to enable it to use non-volatile, or persistent, computer memory. Non-volatile memory (NVM), or persistent memory (PMem), combines the high data transfer rates of the volatile memory with the persistence and resiliency of traditional storage. The virtual NVDIMM device is a virtual NVM device that can retain stored data through reboots or power source failures.

Virtual machines consume the PMem resource of the host through a virtual non-volatile dual in-line memory module (NVDIMM) or through a virtual persistent memory disk.

For more information about persistent memory, see Managing Persistent Memory in the VMware Host Client

Prerequisites

- Verify that the guest OS of the virtual machine supports PMem.
- Verify that the virtual hardware version is 14 or later.
- Verify that you have the **Datastore.Allocate space** privilege.
- Verify that the host or the cluster on which the virtual machine resides has available PMem resources.

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. Under the **Virtual Hardware** tab, click **Add other device** and select **NVDIMM** from the drop-down menu.

   The NVDIMM device appears in the Virtual Hardware devices list. Each virtual machine can have a maximum of 64 NVDIMM devices.
4. Configure the newly added NVDIMM device.
   a. In the Virtual Hardware devices list, expand **New NVDIMM**.
   b. Enter the size of the new NVDIMM device.

      Note You can change the size of the NVDIMM device at a later time. The virtual machine must be powered off.
   c. Select the NVDIMM controller location or leave the default one.
5. Click **Save** to close the wizard.

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 Basics

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

Network Adapter Types

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.

Supported NICs currently differ between an on-premises environment and VMware Cloud on AWS. The following NIC types are supported in an on-premises deployment:

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 Vlance adapter when a virtual machine boots, but initializes itself and functions as either a Vlance or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlance adapter to the higher performance VMXNET adapter.

Vlance

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.

PVRDMA

A paravirtualized NIC that supports remote direct memory access (RDMA) between virtual machines through the OFED verbs API. All virtual machines must have a PVRDMA device and should be connected to a distributed switch. PVRDMA supports VMware vSphere vMotion and snapshot technology. It is available in virtual machines with hardware version 13 and guest operating system Linux kernel 4.6 and later.

For information about assigning an PVRDMA network adapter to a virtual machine, see the *vSphere Networking* documentation.

SR-IOV passthrough

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.

SR-IOV passthrough is available in ESXi 6.0 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.

For information about assigning an SR-IOV passthrough network adapter to a virtual machine, see the *vSphere Networking* documentation.

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

Legacy Network Adapters and ESXi Virtual Hardware Versions

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 use a virtual hardware version, 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.

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 (Optional) Select the adapter type from the **Adapter Type** drop-down menu.

6 Select an option for MAC address configuration.

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

7 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 appears as a single hard disk to the guest operating system. The virtual disk 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 virtual machine data directly on a SAN LUN instead of using a virtual disk file. This option is useful if in your virtual machines you run applications that must detect the physical characteristics of the storage device. Mapping a SAN LUN also allows you to use existing SAN commands to manage storage for the disk.

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

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 later 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. Increasing the size of an Eager Zeroed Thick virtual disk causes a significant stun time for the virtual machine.

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 Standard 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 standard 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.

Add a Persistent Memory Disk in the 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.

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

   The hard disk appears in the Virtual Hardware devices list. By default, the disk is stored on the host-local PMem datastore and you cannot change the datastore.

4 (Optional) Configure the settings for the new hard disk and click **Save** to close the wizard.

   a Expand **New Hard disk**.

   b Enter a value for the hard disk size and select the units from the drop-down menu.

   Note All persistent memory hard disks and NVDIMM modules that you add to the virtual machine share the same PMem resources. So, you must adjust the size of the newly added persistent memory devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

   c From 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.

   d From the **Controller location** drop-down menu, select the location of the controller that the new hard disk uses.

   e 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.

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.

In the vSphere Client, you can add one xHCI controller and one EHCI+UHCI controller. From hardware version 11 to hardware version 16, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeed ports and four logical USB 2.0 ports). With hardware version 17, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeedPlus 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 a VM	Supported for Passthrough from Client Computer to a VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.1, 2.0, and 1.1	Yes USB 3.1, 2.0, and 1.1 devices only.	Yes Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

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

For virtual machines with Windows or Linux guest operating systems, you can add one or two controllers of different types. 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 more than 15 controllers and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- Verify that the ESXi hosts have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices.
- Verify that the client computers have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, verify 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 **Controller location** 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**.

Results

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.

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 appear in the Hardware list.
4. Click 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**.

Add an NVMe Controller in the VMware Host Client

If a virtual machine has multiple hard disks, you can add up to four virtual NVMe controllers to which to assign the disks. Using a NVMe controller significantly reduces the software overhead for processing guest OS I/O, as compared to AHCI SATA or SCSI controllers.

NVMe controllers perform best with virtual disks on an all-flash disk array, local NVMe SSD, and PMem storage.

Prerequisites

- Verify that the virtual machine has a guest operating system that supports NVMe.
- Verify that the virtual machine compatibility is ESXi 6.5 or later.
- Verify that you are familiar with storage controllers behavior and limitations. For more information, see the *Virtual Machine Administration* guide.
- Verify that you have the **Virtual machine.Configuration.Add new disk** 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 Under the **Virtual Hardware** tab, click the **Add other device** icon and select **NVMe controller** from the drop-down menu.

Results

A new NVMe controller is added to the virtual machine.

What to do next

You can add a hard disk to the virtual machine and assign it to the NVMe controller.

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. You can also add a virtual Watchdog Timer (VWDT) device, Precision Clock device, and PCI 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	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	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	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**.

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

By using the VMware Host Client, you can add a USB device to a virtual machine.

Prerequisites

- Verify that a USB controller is present. See Add a USB Controller to a Virtual Machine in the VMware Host Client.
- Add a physical USB device to the ESXi host where the virtual machine is located by plugging the USB device into the host.

Note If the ESXi host does not have available USB devices, you cannot add a USB device to 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 pop-up menu.

3 On the **Virtual Hardware** tab, select **Add other device** and select **USB device** from the drop-down menu.

The USB device appears in the hardware list of available hardware devices for the virtual machine.

4 From the **USB device** drop-down, select which USB device to add to the virtual machine.

5 Click **Save**.

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

By using the VMware Host Client, you can add a sound controller to a 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 **Sound controller** from the drop-down menu.

The sound controller appears in the list of available hardware devices for the virtual machine.

4 From the **Sound card** drop-down menu, select which sound controller to connect to the virtual machine.

5 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.

Option	Description
Use named pipe	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	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. Expand the parallel port and in the Connection field, browse to a folder to create the file in.

   The file path appears in the **Connection** text box.
5. (Optional) Select **Connect at power on** to configure the device to connect when the virtual machine powers on.
6. Click **Save**.

Using a Virtual Watchdog Timer

To ensure self-reliance related to the system performance within a virtual machine, you can add a virtual Watchdog Timer (VWDT) device. If the guest operating system stops responding and cannot recover on its own due to software glitches or errors, the VWDT waits for a predefined period of time and then restarts the system.

You can enable the VWDT to start either by the guest operating system, or by the BIOS or EFI firmware. If you chose the VWDT to start by the BIOS or EFI firmware, it starts before the guest operating system boots.

The VWDT has an important role in guest-based clustering solutions where each virtual machine in the cluster can recover on its own if it fails.

Add a Virtual Watchdog Timer Device to a Virtual Machine in the VMware Host Client

You can add a virtual Watchdog Timer device to a virtual machine to prevent the virtual machine from a guest operating system failure for an extended period of time.

Prerequisites

- Power off the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.
- Verify that the guest operating system of the virtual machine supports the VWDT device.
- Verify that the virtual hardware version is 17.

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 click **Watchdog Timer**.

   The Watchdog Timer device appears in the hardware list.

4 (Optional) Select **Start with BIOS/EFI boot** to start the watchdog timer by the BIOS or EFI firmware.

   When you select this option, the VWDT device starts before the guest operating system. If the Guest OS boot takes too long or does not support the watchdog timer, the device might constantly restart the virtual machine.

5 Click **Save**.

Add a Precision Clock Device to a Virtual Machine in the VMware Host Client

A precision clock is a virtual device that runs on a virtual machine and accesses the system time of a host. By adding a precision clock to a virtual machine, you ensure time synchronization and high precision timestamping.

Prerequisites

- Power off the virtual machine.
- Verify that the virtual hardware version is 17.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Modify device settings** privilege on the virtual machine.

Procedure

1 In the VMware Host Client inventory, click **Virtual Machines**.

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 **Precision Clock**.

   The precision clock device appears in the hardware list.

4 (Optional) Select the time synchronization protocol.

5 Click **Save**.

Add a PCI Device to a Virtual Machine in the VMware Host Client

DirectPath I/O allows the guest operating system of a virtual machine to access the physical PCI and PCIe devices connected to a host directly. By using this technology, you can connect each virtual machine to up to sixteen physical PCI devices. You can use Dynamic DirectPath I/O to assign multiple PCI passthrough devices to a virtual machine. Starting with vSphere 7.0, you can identify the PCI passthrough devices by their vendor and model name.

Note Some virtual machine operations become unavailable when you add a PCI or PCIe passthrough device to the virtual machine.

For information about the hardware label configuration, see Change the Hardware Label in the VMware Host Client.

Prerequisites

- Power off the virtual machine.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.
- Verify that the PCI devices are connected to the host and marked as available for passthrough.
- If you want to add a dynamic PCI device to a virtual machine, verify that the virtual hardware version is 17.

Procedure

1 In the VMware Host Client inventory, click **Virtual Machines**.

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 a device.

Option	Action
PCI device	a Click **PCI device**. A new device appears in the hardware list. b From the drop-down menu, select a PCI device to connect to the virtual machine.
Dynamic PCI device	a Click **Dynamic PCI device**. A new device appears in the hardware list. b Expand **New PCI device**, and from the drop-down menu, select the PCI passthrough devices to connect to the virtual machine. You can identify PCI passthrough devices by vendor, model name, and hardware label. Hardware labels, if present, are displayed in brackets. **Note** When you add a PCI device to a virtual machine, the full memory size of the virtual machine is automatically reserved.

4 Click **Save**.

Securing Virtual Machines with Intel Software Guard Extensions

By using the vSphere Client, you can configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines and provide additional security to your workloads.

Some modern Intel CPUs implement a security extension called Intel® Software Guard Extensions (Intel SGX). Intel SGX is a processor-specific technology that defines private regions of memory, called enclaves. Intel SGX protects the enclave contents from disclosure and modification in such a way that code running outside the enclave cannot access them.

vSGX enables virtual machines to use Intel SGX technology if available on the hardware. To use vSGX, the ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the BIOS of the ESXi host. You can use the vSphere Client to enable SGX for a virtual machine.

Enable vSGX on a Virtual Machine in the VMware Host Client

To protect the enclave contents from disclosure and modifications, you can enable vSGX on a virtual machine in the VMware Host Client.

Some operations and features are not compatible with SGX.

- Migration with Storage vMotion
- Suspending or resuming the virtual machine
- Taking a snapshot of the virtual machine
- Fault Tolerance
- Enabling Guest Integrity (GI, platform foundation for VMware AppDefense 1.0)

Prerequisites

- Power off the virtual machine.
- Verify that the virtual machine uses EFI firmware.
- Verify that the ESXi host is version 7.0 or later.
- Verify that the guest operating system in the virtual machine is Linux, Windows 10 (64-bit) or later, or Windows Server 2016 (64-bit) or later.
- Verify that you have the **Virtual machine.Configuration.Modify device settings** privilege on the virtual machine.
- Verify that the ESXi host is installed on an SGX-capable CPU, and SGX is enabled in the BIOS of the ESXi host. For information about the supported CPUs, see https://kb.vmware.com/s/article/71367.

Procedure

1. In the VMware Host Client inventory, click **Virtual Machines**.
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 **Security devices**.
4. Select the **Enable** check box.
5. Under **Enclave page cache size**, enter a new value in the text box and select the size in MB or GB from the drop-down menu.

   Note The enclave page cache size must be a multiple of 2.

6 From the **Launch control configuration** drop-down menu, select the appropriate mode.

Option	Action
Locked	Enables the launch enclave configuration. Under **Launch enclave public key hash**, enter a valid SHA256 hash. The SHA256 hash key must contain 64 characters.
Unlocked	Enables the launch enclave configuration of the guest operating system.

7 Click **Save**.

Disable vSGX on a Virtual Machine in the VMware Host Client

To disable vSGX on a virtual machine, you can use the VMware Host Client.

Procedure

1 In the VMware Host Client inventory, click **Virtual Machines**.

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 **Security devices**.

4 Deselect the **Enable** check box and click **Save**.

Results

vSGX is disabled on the virtual machine.

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.

Results

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.

Power States of a Virtual Machine in the VMware Host Client

The basic power operations for a virtual machine include powering on, powering off, suspending, and reset.

For information about how to change the virtual machine power states, see Configure the Virtual Machine Power States in the VMware Host Client.

Prerequisites

- Verify that you have the **VirtualMachine.Interaction.PowerOn** privilege.
- Verify that you have the **VirtualMachine.Interaction.PowerOff** privilege.
- Verify that you have the **VirtualMachine.Interaction.Suspend** privilege.
- Verify that you have the **VirtualMachine.Interaction.Reset** privilege.

Procedure

1 In the VMware Host Client inventory, click **Virtual Machines**.

2 Right-click a virtual machine and select a power operation.

Option	Description
Power On (▶)	Powers on a virtual machine when the virtual machine is stopped.
Power off (🟥)	Powers off a virtual machine and shuts down the guest operating system. Powering off a virtual machine might cause loss of data.
Suspend (⏸)	Suspends a running virtual machine and leaves it connected to the network. When you resume a suspended virtual machine, the virtual machine continues operating at the same point the virtual machine was at when it was suspended.
Reset (🔄)	Shuts down and restarts the guest operating system without powering off the virtual machine.

Use Virtual Machine Column Configuration in the VMware Host Client

The virtual machines panel in the VMware Host Client allows you to configure the information that you want to display. You can show or hide different columns, such as status, used space, host name, host CPU, and so on.

Procedure

1 Click **Virtual Machines** in the VMware Host Client inventory.

2 In the list of virtual machines, click the down arrow icon next to any column title and select **Select columns**.

   The list with all available columns appears.

3 Select the information that you want to display 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**.

Results

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

Remove Virtual Machines from a Datastore in the VMware Host Client

To free space on the datastore, you can remove the virtual machines that you no longer need. Removing a virtual machine from the VMware Host Client inventory deletes all virtual machine files from the datastore, including the configuration file and virtual disk files. You can delete multiple virtual machines

Prerequisites

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

Procedure

1 Click **Virtual Machines** in the VMware Host Client inventory.

2 Select one or multiple check boxes next to the virtual machines that you want to remove and select **Actions > Delete**.

   The **Delete VMs** dialog box opens.

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 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 extra 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, the guest operating system stops writing to it, and a delta or child disk is created.

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

The files that make up the delta disk are called child disks or redo logs.

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 ESXi host takes to write the memory onto the disk depends on 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
vmname-number.vmdk and *vmname-number*-delta.vmdk	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. The filename uses the following syntax, `S1vm-000001.vmdk` where `S1vm` is the name of the virtual machine and the six-digit number, `000001`, 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.
vmname.vmsd	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
vmname.Snapshot*number*.vmsn	Memory state of the virtual machine at the time you take the snapshot. The filename uses the following syntax, `S1vm.snapshot1.vmsn`, where `S1vm` is the virtual machine name, and `snapshot1` is the first snapshot. **Note** A `.vmsn` file is created each time you take a snapshot, regardless of the memory selection. A `.vmsn` file without memory is much smaller than one with memory.

Snapshot Limitations

Snapshots can affect the 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.
- Quiesced snapshots require VMware Tools installation and guest operating system support.
- Snapshots are not supported with PCI vSphere DirectPath 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 if there is 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 2 TB, snapshot operations can take much 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 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. 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 and select **Snapshots > Take snapshot**.
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 **Take snapshot**.

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 the Latest 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 and select **Snapshots > Restore snapshot**.

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

3 Click **Restore** 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 large amount of information needs to be read and written to a disk. This process 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.

Note Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other 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 and select **Snapshots > Manage Snapshots**.

3 Click the snapshot that you want to delete and click **Delete snapshot**.

4 (Optional) In the **Delete Snapshot** dialog box, select the **Remove all children snapshots** check-box to delete the selected snapshot together with all its children snapshots.

5 Click **Remove** to confirm the deletion.

6 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 a notification to view details.

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

Securing Virtual Machines in the VMware Host Client

The guest operating system that runs in the virtual machine is vulnerable to the same security risks as any physical system. To boost security in your virtual environment, you can add a virtual Trusted Platform Module (vTPM) to your ESXi hosts. You can also enable virtualization-based security (VBS) for the virtual machines that run the latest Windows 10 and Windows Server 2016 operating systems.

Using Virtual TPM in the VMware Host Client

The Trusted Platform Module (TPM) is a specialized chip that stores host-specific sensitive information, for example private keys and OS secrets. The TPM chip is also used to perform cryptographic tasks and attest the integrity of the platform.

The virtual TPM device is a software emulation of the TPM functionality. You can add a virtual TPM (vTPM) device to the virtual machines in your environment. The vTPM implementation does not require a physical TPM chip on the host. ESXi uses the vTPM device to exert the TPM functionality in your vSphere environment.

vTPM is available to virtual machines that have Windows 10 and Windows Server 2016 operating systems. The virtual machine must be of hardware version 14 or later.

You can add a virtual TPM device to a virtual machine only in the vCenter Server instance. For more information, see the *vSphere Security* documentation.

In the VMware Host Client, you can only remove the virtual TPM device from a virtual machine.

Using VBS in the VMware Host Client

Virtualization-based security (VBS) uses the Microsoft Hyper-V based virtualization technology to isolate core Windows OS services in a separate virtualized environment. Such isolation provides an additional level of protection, because it makes it impossible for the key services in your environment to be manipulated.

Enabling VBS on a virtual machine automatically enables the virtual hardware that Windows requires for the VBS feature. By enabling VBS, a variant of Hyper-V starts in the virtual machine and Windows starts running inside the Hyper-V root partition.

VBS is available on the latest Windows OS versions, for example Windows 10 and Windows Server 2016. To use VBS on a virtual machine, the virtual machine compatibility must be ESXi 6.7 and later.

In the VMware Host Client, you can enable VBS during a virtual machine creation. Alternatively, you can enable or disable VBS for an existing virtual machine.

Note You can enable VBS on a virtual machine only if the TPM validation of the host is successful.

Remove a vTPM device from a VM in the VMware Host Client

In the VMware Host Client, you can only remove the vTPM device from a virtual machine.

Prerequisites

- The virtual machine must be of hardware version 14 or later.
- The guest OS must be Windows 10 or Windows Server 2016 and later.
- The virtual machine must be powered off.

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, find the TPM device and click the **Remove** icon.

   The virtual TPM device is removed from the virtual machine.
4. Click **Save** to close the wizard.

Enable or Disable Virtualization-based Security on an Existing VM in the Host Client

You can change the level of security of a virtual machine by enabling or disabling Microsoft virtualization-based security (VBS) on existing virtual machines for supported Windows guest operating systems.

Prerequisites

Using Intel CPUs for VBS requires vSphere 6.7 or later. The virtual machine must have been created using hardware version 14 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit)
- Windows Server 2016 (64 bit)
- Windows Server 2019 (64 bit)

Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later. The virtual machine must have been created using hardware version 18 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit), version 1809

- Windows Server 2019 (64 bit)

Ensure that you install the latest patches for Windows 10, version 1809, and Windows Server 2019, before enabling VBS.

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, enable or disable VBS for the virtual machine.

   - To enable VBS for the virtual machine, select the **Enable Virtualization Based Security** check box.
   - To disable VBS for the virtual machine, deselect the **Enable Virtualization Based Security** check box.

   When you enable VBS, several options are automatically selected and become dimmed in the wizard.

4 Click **Save** to close the wizard.

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

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.

Create 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. 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.
3. On the Select creation type page, select **Create new VMFS datastore** and click **Next**.

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

4. On the Select device page, select where to create the new VMFS partition.
   a. Enter a name for the new datastore.
   b. Select a device to add the datastore to.

      The list contains only devices that have enough available space.
   c. Click **Next**.
5. On the Select partitioning options page, select how to partition the device and click **Next**.

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.

6. On the Ready to complete page, review the configuration details 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 an extent.

Use one of the following methods to increase the 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 the extent. The datastore can span over up to 32 extents with the size of each extent of more than 2 TB, yet appear as a single volume. The spanned VMFS datastore can use any or all its extents at any time. It does not need to fill up a particular extent before using the next one.

  Note Datastores that support only the hardware assisted locking, also called the atomic test and set (ATS) mechanism, cannot span over non-ATS devices. For more information, see *vSphere Storage*.

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. On the Select creation type page, click **Add an extent to existing VMFS datastore** and click **Next**.
4. On the Select datastore page, select the datastore to expand and click **Next**.
5. On the Select device page, select a device to create the new VMFS partition on and click **Next**.
6. On the Select partitioning options page, select how to partition the device and click **Next**.

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.

7. On the Ready to complete page, review the configuration details 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. 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. vSphere supports versions 3 and 4.1 of the NFS protocol.

The ESXi host can mount an NFS volume and use it for its storage needs.

Typically, the NFS volume or directory is created by a storage administrator and is exported from the NFS server. You do not need to format the NFS volume with a local file system, such as VMFS. Instead, you mount the volume directly on the ESXi hosts and use it to store and boot virtual machines in the same way that you use the 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 the ISO images, you can connect the CD-ROM device of the virtual machine to an ISO file on the datastore. You then can install a guest operating system from the ISO file.

When you use NFS storage, follow the specific guidelines related to NFS server configuration, networking, NFS datastores, and so on.

Procedure

1 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.

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 On the Select creation type page, click **Mount NFS datastore** and click **Next**.

4 On the Provide NFS mount details page, provide the details for the NFS you mount.

   a Enter a name for the NFS datastore.

   b 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.

   c Specify the NFS share.

   d Specify the NFS version.

   e Click **Next**.

5 On the Ready to complete page, review the configuration 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 unmounting 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.
- Storage DRS does not manage the datastore.
- 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 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 **Datastore browser**.
3. Select the datastore that you want to store the file on.
4. (Optional) Click **Create directory** to 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 **Datastore 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 **Datastore 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 **Datastore 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 **Datastore 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 **Datastore 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.

Note If the host is managed by vCenter Server, you cannot rename the datastore from the VMware Host Client. You can only perform the task from the vCenter Server instance that manages the host.

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 systems. The host can offload certain virtual machine and storage management operations to the storage systems. With the storage hardware assistance, your host performs these operations faster and consumes less CPU, memory, and storage fabric bandwidth.

Block storage devices, Fibre Channel and iSCSI, and NAS devices support the hardware acceleration.

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.

Managing Storage Adapters in the VMware Host Client

When you connect to a host or to vCenter Server by using the VMware Host Client, you can perform various tasks on your storage adapters, such as configuring various iSCSI components.

When you enable iSCSI on the host that you are managing in your VMware Host Client environment, you can configure and add new network port bindings, static and dynamic targets, you can manage CHAP authentication, and configure various advanced settings on your host storage.

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.

Configuring Software iSCSI Adapters in the VMware Host Client

With the software-based iSCSI implementation, you can use standard NICs to connect your host to a remote iSCSI target on the IP network. The software iSCSI adapter that is built into ESXi communicates with the physical NICs through the network stack.

Note Before you can use the software iSCSI adapter, you must set up networking, activate the adapter, and configure parameters such as CHAP.

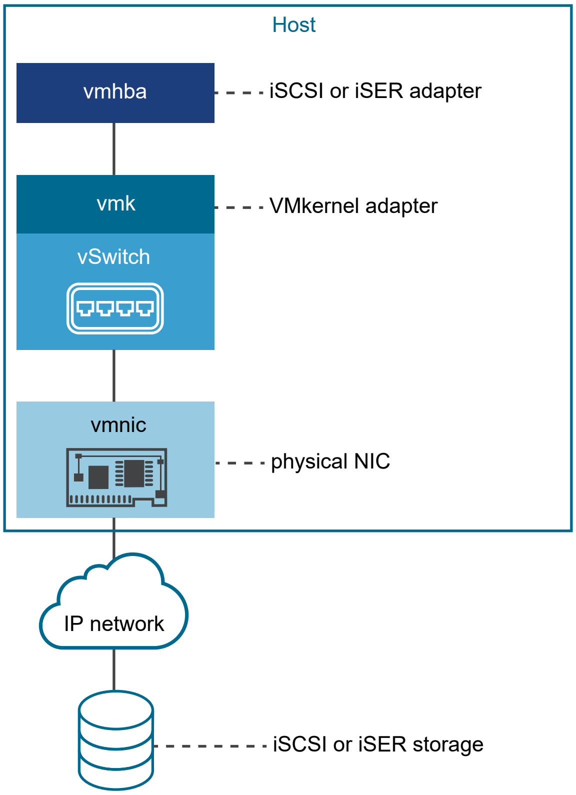
The iSCSI adapter configuration workflow includes the following procedures:

- Enabling iSCSI on your host. SeeEnable iSCSI for an ESXi Host in the VMware Host Client.
- Adding a port binding. See Add Port Binding in the VMware Host Client.
- Removing port binding. See Remove Port Binding in the VMware Host Client.

Setting Up Network for iSCSI and iSER

Certain types of iSCSI adapters depend on the VMkernel networking. These adapters include the software or dependent hardware iSCSI adapters, and the VMware iSCSI over RDMA (iSER) adapter. If your environment includes any of these adapters, you must configure connections for the traffic between the iSCSI or iSER component and the physical network adapters.

Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter. You then associate the VMkernel adapter with an appropriate iSCSI or iSER adapter. This process is called port binding.



Follow these rules when configuring the port binding:

- You can connect the software iSCSI adapter with any physical NICs available on your host.
- The dependent iSCSI adapters must be connected only to their own physical NICs.
- You must connect the iSER adapter only to the RDMA-capable network adapter.

For specific considerations on when and how to use network connections with software iSCSI, see the VMware knowledge base article at http://kb.vmware.com/kb/2038869.

Enable iSCSI for an ESXi Host in the VMware Host Client

Enable iSCSI for your host in your VMware Host Client environment to configure storage adapters parameters, such as CHAP authentication, network port bindings, static and dynamic targets, and various advanced settings.

Procedure

1. Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.
2. Select the **Enabled** radio button.
3. (Optional) Configure the parameters and components that you want to change.
4. Click **Save configuration**.

Best Practices for Configuring Networking with Software iSCSI

When you configure networking with software iSCSI, consider several best practices.

Software iSCSI Port Binding

You can bind the software iSCSI initiator on the ESXi host to a single or multiple VMkernel ports, so that iSCSI traffic flows only through the bound ports. Unbound ports are not used for iSCSI traffic.

When port binding is configured, the iSCSI initiator creates iSCSI sessions from all bound ports to all configured target portals.

See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 bound VMkernel ports	2 target portals	4 sessions (2 x 2)
4 bound VMkernel ports	1 target portal	4 sessions (4 x 1)
2 bound VMkernel ports	4 target portals	8 sessions (2 x 4)

Note Make sure that all target portals are reachable from all VMkernel ports when port binding is used. Otherwise, iSCSI sessions might fail to create. As a result, the rescan operation might take longer than expected.

No Port Binding

If you do not use port binding, the ESXi networking layer selects the best VMkernel port based on its routing table. The host uses the port to create an iSCSI session with the target portal. Without the port binding, only one session per each target portal is created.

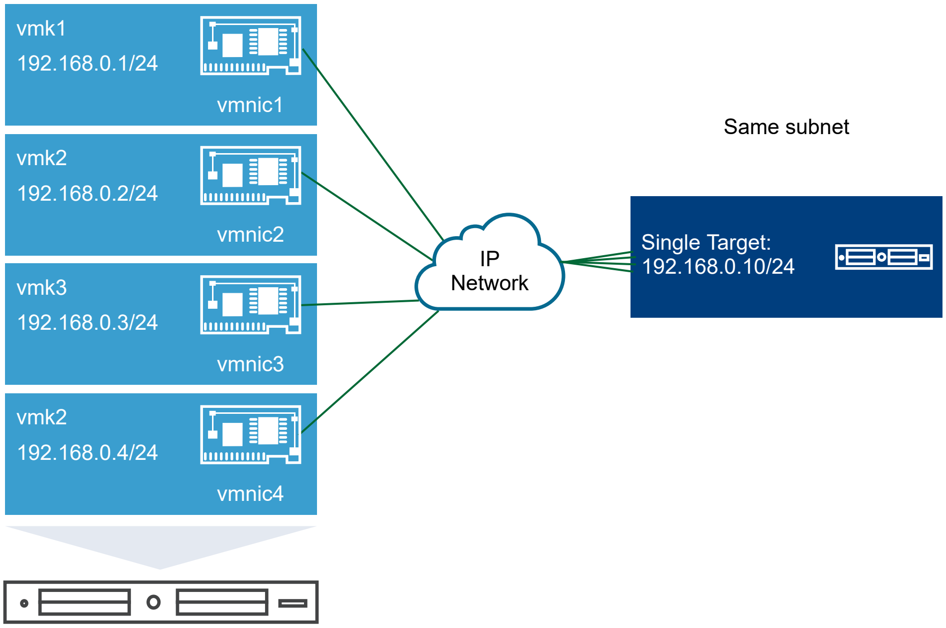
See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 unbound VMkernel ports	2 target portals	2 sessions
4 unbound VMkernel ports	1 target portal	1 session
2 unbound VMkernel ports	4 target portals	4 sessions

Software iSCSI Multipathing

Example 1. Multiple paths for an iSCSI target with a single network portal

If your target has only one network portal, you can create multiple paths to the target by adding multiple VMkernel ports on your ESXi host and binding them to the iSCSI initiator.

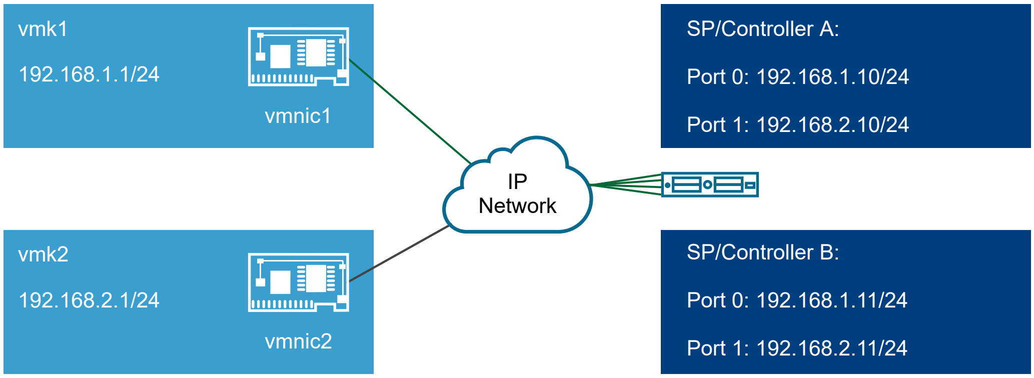


In this example, all initiator ports and the target portal are configured in the same subnet. The target is reachable through all bound ports. You have four VMkernel ports and one target portal, so total of four paths are created.

Without the port binding, only one path is created.

Example 2. Multiple paths with VMkernel ports in different subnets

You can create multiple paths by configuring multiple ports and target portals on different IP subnets. By keeping initiator and target ports in different subnets, you can force ESXi to create paths through specific ports. In this configuration, you do not use port binding because port binding requires that all initiator and target ports are on the same subnet.



ESXi selects vmk1 when connecting to Port 0 of Controller A and Controller B because all three ports are on the same subnet. Similarly, vmk2 is selected when connecting to Port 1of Controller A and B. You can use NIC teaming in this configuration.

Total of four paths are created.

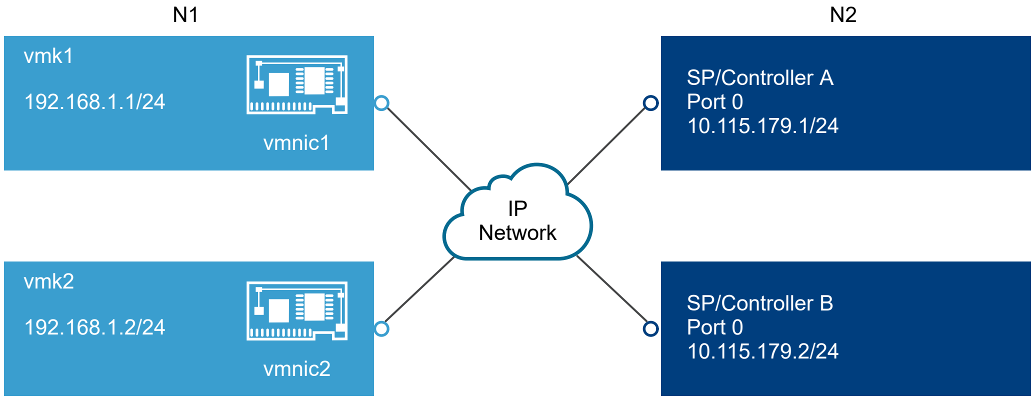
Paths	Description
Path 1	vmk1 and Port0 of Controller A
Path 2	vmk1 and Port0 of Controlled B
Path 3	vmk2 and Port1 of Controller A
Path 4	vmk2 and Port2 of Controller B

Routing with Software iSCSI

You can use the `esxcli` command to add static routes for your iSCSI traffic. After you configure static routes, initiator and target ports in different subnets can communicate with each other.

Example 1. Using static routes with port binding

In this example, you keep all bound vmkernel ports in one subnet (N1) and configure all target portals in another subnet (N2). You can then add a static route for the target subnet (N2).

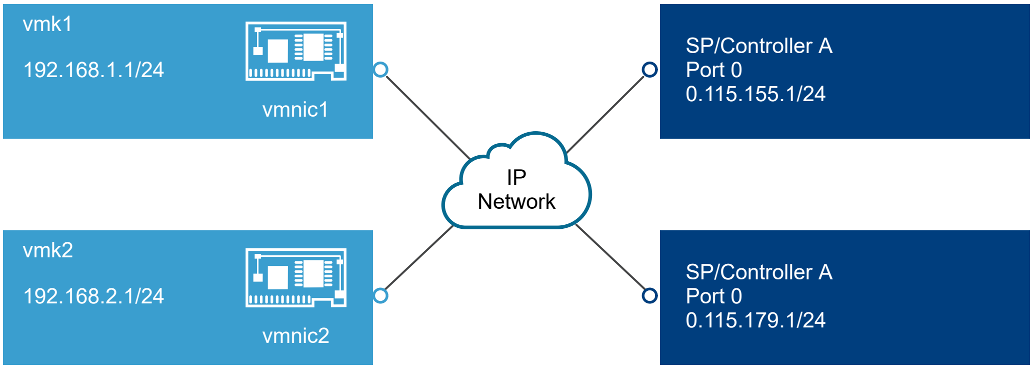


Use the following command:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Example 2. Using static routes to create multiple paths

In this configuration, you use static routing when using different subnets. You cannot use the port binding with this configuration.



You configure vmk1 and vmk2 in separate subnets, 192.168.1.0 and 192.168.2.0. Your target portals are also in separate subnets, 10.115.155.0 and 10.155.179.0.

You can add the static route for 10.115.155.0 from vmk1. Make sure that the gateway is reachable from vmk1.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.155.0/24
```

You then add static route for 10.115.179.0 from vmk2. Make sure that the gateway is reachable from vmk2.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network
10.115.179.0/24
```

When connecting with Port 0 of Controller A, vmk1 is used.

When connecting with Port 0 of Controller B, vmk2 is used.

Example 3. Routing with a separate gateway per vmkernel port

Starting with vSphere 6.5, you can configure a separate gateway per VMkernel port. If you use DHCP to obtain IP configuration for a VMkernel port, gateway information can also be obtained using DHCP.

To see gateway information per VMkernel port, use the following command:

```
# esxcli network ip interface ipv4 address list
```

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

With separate gateways per VMkernel port, you use port binding to reach targets in different subnets.

Add Port Binding in the VMware Host Client

Use the VMware Host Client to bind an iSCSI adapter with a VMkernel adapter on your host.

Prerequisites

- Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.
- Required privilege:**Host.Configuration.Storage Partition Configuration**

Procedure

1. Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.
2. In the **Network port bindings** section, click **Add port binding**.

3 Select a VMkernel adapter to bind with the iSCSI adapter.

Note Make sure that the network policy for the VMkernel adapter is compliant with the binding requirements.

You can bind the software iSCSI adapter to one or more VMkernel adapters. For a dependent hardware iSCSI adapter, only one VMkernel adapter associated with the correct physical NIC is available.

4 Click **Select**.

5 Click **Save configuration**.

Remove Port Binding in the VMware Host Client

Edit the iSCSI configuration on your host to remove a port binding.

Procedure

1 Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.

2 In the **Network port bindings** section, select a VMkernel NIC from the list.

3 Click **Remove port binding**.

4 Click **Save configuration**.

Configuring Discovery Addresses for iSCSI Adapters

You need to set up target discovery addresses, so that the iSCSI adapter can determine which storage resource on the network is available for access.

The ESXi system supports these discovery methods:

Dynamic Discovery

Also known as SendTargets discovery. Each time the initiator contacts a specified iSCSI server, the initiator sends the SendTargets request to the server. The server responds by supplying a list of available targets to the initiator. The names and IP addresses of these targets appear on the **Static Discovery** tab. If you remove a static target added by dynamic discovery, the target might be returned to the list the next time a rescan happens, the iSCSI adapter is reset, or the host is rebooted.

Note With software and dependent hardware iSCSI, ESXi filters target addresses based on the IP family of the iSCSI server address specified. If the address is IPv4, IPv6 addresses that might come in the SendTargets response from the iSCSI server are filtered out. When DNS names are used to specify an iSCSI server, or when the SendTargets response from the iSCSI server has DNS names, ESXi relies on the IP family of the first resolved entry from DNS lookup.

Static Discovery

In addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets. The iSCSI adapter uses a list of targets that you provide to contact and communicate with the iSCSI servers.

Set Up a Static Target in the VMware Host Client

With iSCSI initiators, you can use static discovery to manually enter information for the targets.

When you set up Static Discovery, you can only add new iSCSI targets. You cannot change the IP address, DNS name, iSCSI target name, or port number of an existing target. To make changes, remove the existing target and add a new one.

Prerequisites

Required privileges: **Host.Configuration.Storage Partition Configuration**

Procedure

1. Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.
2. Click **Add static target**.

   The new static target appears in the list.
3. To add a name for the new static target, click the target in the list and enter the name.
4. To add an address for the new static target, click the target in the list and type the address.
5. (Optional) To change the port number of the new static target, click the target **Port** text box and type the new port number.
6. (Optional) To edit the static target settings, select the new target from the list of available targets, click **Edit settings**, configure the parameters that you want to change, and click **Save**.
7. (Optional) To delete a specific target, select the target and click **Remove static target**.

   The target no longer appears in the list of existing static targets.
8. Click **Save configuration**.

Set up a Dynamic Target in the VMware Host Client

With Dynamic Discovery, each time the initiator contacts a particular iSCSI storage system, the initiator sends the SendTargets request to the iSCSI system. The iSCSI system responds by supplying a list of available targets to the initiator.

When you set up Dynamic Discovery, you can only add a new iSCSI system. You cannot change the IP address, DNS name, or port number of an existing iSCSI system. To modify the parameters, delete the existing system and add a new one.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

1 Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.

2 Click **Add dynamic target**.

The new dynamic target appears in the list.

3 To add an address for the new dynamic target, click the target in the list and enter the address .

4 (Optional) To change the port number of the new dynamic target, click the target **Port** text box and enter the new port number.

5 (Optional) To edit the dynamic target settings, select the new target from the list of available targets, click **Edit settings**, configure the parameters that you want to change, and click **Save**.

6 (Optional) To delete a specific target, select the target and click **Remove dynamic target**.

The target no longer appears in the list of existing dynamic targets.

7 Click **Save configuration**.

Edit Advanced Settings for iSCSI in the VMware Host Client

The advanced iSCSI settings control such parameters as header and data digest, ARP redirection, delayed ACK, and so on. Generally, you do not need to change these settings because your host works with the assigned predefined values.

Caution Do not change the advanced iSCSI settings unless you are working with the VMware support team or otherwise have thorough information about the values to provide for the settings modification.

Prerequisites

Required privilege: **Host.Configuration.Storage Partition Configuration**

Procedure

1 Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.

2 Click **Advanced settings** to display the entire list of settings.

3 Edit the parameters that you want to change and click **Save configuration**.

Set Up CHAP Authentication for an iSCSI Adapter in the VMware Host Client

You can set up all targets to receive the same CHAP name and secret from the iSCSI initiator at the initiator level. By default, all discovery addresses or static targets inherit the CHAP parameters that you set up at the initiator level.

The CHAP name must be fewer than 511 alphanumeric characters and the CHAP secret must be fewer than 255 alphanumeric characters. Some adapters, for example the QLogic adapter, might have lower limits, 255 for the CHAP name and 100 for the CHAP secret.

Prerequisites

- Before you set up CHAP parameters for software or dependent hardware iSCSI, determine whether to configure one-way, also known as normal, or mutual CHAP. Independent hardware iSCSI adapters do not support mutual CHAP.
  - In one-way CHAP, the target authenticates the initiator.
  - In mutual CHAP, both the target and the initiator authenticate each other. Use different secrets for CHAP and mutual CHAP.

  When you configure CHAP parameters, verify that they match the parameters on the storage side.
- Required privileges: **Host.Configuration.Storage Partition Configuration**

Procedure

1 Click **Storage** in the VMware Host Client inventory, click **Adapters**, and click **Configure iSCSI**.

2 To configure one-way CHAP, expand **CHAP authentication** to display all parameters.

   a Select the CHAP security level.

   b Enter the CHAP name.

   Make sure that the name you enter matches the name configured on the storage side.

   c Enter a one-way CHAP secret to use for authentication. Use the same secret that you enter on the storage side.

3 To configure mutual CHAP, select **Use CHAP** as an option for one-way CHAP. Expand **Mutual CHAP authentication** to display all parameters.

   a Select **Use CHAP**.

   b Enter the mutual CHAP name.

   c Enter the mutual CHAP secret.

   Use different secrets for the one-way CHAP and the mutual CHAP.

4 Click **Save configuration**.

Results

If you change the authentication settings for an iSCSI adapter, you only use the updated credentials for new iSCSI sessions. Existing sessions persist until either the connection is lost due to some outside factor, such as force re-authentication, or you remove and add the adapter iSCSI targets.

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 vSAN.

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 vSAN.

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.

Managing Persistent Memory in the VMware Host Client

ESXi 6.7 provides support for the latest computer memory technology, which is called non-volatile memory (NVM) or persistent memory (PMem). PMem combines the high data transfer rate of volatile computer memory with the persistence and resiliency of traditional storage. PMem devices have low access latency and can retain stored data through reboots or power outages.

Modes of Consumption of the Persistent Memory Resources of the Host

When you add a physical PMem device to a host, ESXi detects the PMem resource and exposes it as a host-local PMem datastore to the virtual machines that run on the host. Depending on the guest operating system, virtual machines can have direct access to the PMem resources.

Each host can have only one local PMem datastore that pools and represents all PMem resources of the host.

Persistent memory combines the properties of both memory and storage. So, virtual machines can consume the PMem resources of the ESXi host as memory (through virtual NVDIMM devices) or as storage (through virtual PMem hard disks).

The host-local PMem datastore stores all direct-accessed NVDIMM devices and virtual PMem hard disks.

Virtual PMem (vPMem)

In this mode, if the guest operating system is PMem-aware, the virtual machine can have direct access to the physical PMem resources of the host and use them as standard, byte-addressable memory.

Virtual machines use virtual non-volatile dual in-line memory modules (NVDIMMs) for direct access to PMem. The NVDIMM is a memory device that sits on an ordinary memory channel, but contains non-volatile memory. In vSphere 6.5, the virtual NVDIMM is a new type of device that represents the physical PMem regions of the host. A single virtual machine can have up to 64 virtual NVDIMM devices. Each NVDIMM device is stored on the host-local PMem datastore.

Note To add an NVDIMM device to a virtual machine, the virtual machine must be of hardware version 14 and the guest operating system must support persistent memory. If the guest operating system is not PMem-aware, you can still use PMem, but you cannot add an NVDIMM device to the virtual machine.

Virtual PMem Disks (vPMemDisk)

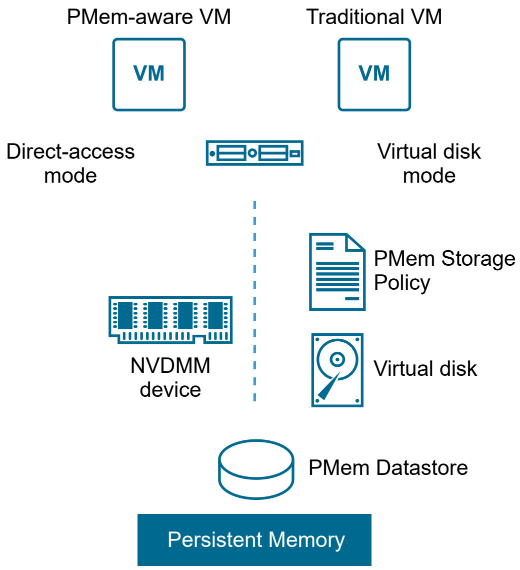
In this mode, the virtual machine does not have direct access to the PMem resources of the host.

You must add a virtual PMem hard disk to the virtual machine. A virtual PMem hard disk is a traditional SCSI disk to which the PMem Storage Policy is applied. The policy automatically places the hard disk on the host-local PMem datastore.

In this mode of usage, there are no requirements for the hardware version of the virtual machine and the guest operating system.

Note If the guest operating system is not PMem-aware, virtual machines can use PMem only through vPMemDisks.

The following graphic illustrates how the persistent memory components interact.



For information about how to configure and manage VMs with NVDIMMs or virtual persistent memory disks, see the *vSphere Resource Management* documentation.

Structure of the PMem Datastore

The VMware Host Client user interface provides information about the complex structure of the host-local PMem datastore. If you want to analyze this information and use it for troubleshooting and management purposes, you must be familiar with the concepts related to that complex structure.

Modules

In the VMware Host Client user interface, modules represent the physical NVDIMMs that are connected to the motherboard of the host.

In the VMware Host Client, you can check the health status of each module and identify unhealthy NVDIMM modules.

Interleave Sets

Interleave sets are logical groupings of one or multiple modules. Interleave sets reveal how information is spread across the physical DIMMs and how ESXi reads the information from the modules. Because ESXi reads from each interleave set in turns, interleave sets ensure higher memory throughput.

For example, if an interleave set consists of two modules, ESXi reads the information from the two physical DIMMs in parallel and then proceeds with the next interleave set.

The VMware Host Client user interface provides information about the way NVDIMMS are grouped into interleave sets.

Namespaces

Namespaces are regions of contiguously addressed memory ranges in the NVDIMM. Namespaces can go across interleave sets. The PMem datastore is built on top of the namespaces.

In the VMware Host Client, you can view the capacity, health status, and the location ID of every namespace.

View Information About Modules, Interleave Sets, and Namespaces in the VMware Host Client

In the VMware Host Client you can view information about the modules, interleave sets, and namespace of the host-local PMem datastore. As a result, you can easily identify an unhealthy module and perform troubleshooting.

You cannot perform most of the traditional datastore management tasks on the host-local PMem datastore. However, you can use the information about modules, interleave sets, and namespaces for troubleshooting purposes.

Prerequisites

Verify that the host has at least one physical NVDIMM device.

Procedure

1 In the **Navigator** pane, click **Storage**.

2 On the **Persistent Memory** tab, view information about the host-local PMem datastore.

   - Click **Modules** to view information about the NVDIMMs that make up the PMem datastore.
   - Click **Namespaces** to view information about namespaces on the NVDIMMs.
   - Click **Interleave sets** to see how the modules, or physical NVDIMMs, are grouped into interleave sets.

Delete a Namespace in the VMware Host Client

In the VMware Host Client, you can delete namespaces that were not created by ESXi, but by an OS that was previously installed on the host machine.

Prerequisites

- Put the host in maintenance mode.
- Back up the content of the namespace if you might need that content at a later time.

Procedure

1. In the VMware Host Client, click **Storage**.
2. Under the **Persistent Memory** tab, click **Namespaces**.
3. (Optional) In the list of namespaces, check the State column to determine which namespaces ESXi currently uses.

   To free up space, you must delete namespaces whose state is In Use.
4. Select a namespace and click the **Delete** icon.

   Important Deleting a namespace frees up space on the datastore, but you can use the free space only after you reboot the host.
5. Click the **Reboot host** icon to reboot the host.

Results

The selected namespace is deleted from the PMem datastore. ESXi automatically creates a new namespace that the PMem datastore can use. The new namespace has the same capacity, type, and location ID as the deleted one.

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, and events and tasks associated with that datastore. Starting with vSphere 6.5 Update 1 and after you enable the vSAN service in the vSphere Client, you can also monitor your vSAN environment.

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.
5. (Optional) Click **Events** to view events associated with the datastore.
6. (Optional) Click **vSAN** to view the configuration parameters of the vSAN environment of your host.
7. (Optional) Click **Hosts** to view the hosts that reside on this datastore.

8 (Optional) Click **Health** to view details about the status of various parameters, such as **Performance service**, **Network**, **Physical disk**, **Data**, **Cluster**, and **Limits**.

Monitoring vSAN in the VMware Host Client

You can use the VMware Host Client to monitor the vSAN environment of your ESXi host.

vSAN Concepts

VMware vSAN uses a software-defined approach that creates shared storage for virtual machines. It virtualizes the local physical storage resources of ESXi hosts. It also turns them into pools of storage that can be divided and assigned to virtual machines and applications according to their quality-of-service requirements. vSAN is implemented directly in the ESXi hypervisor.

You can configure vSAN to work as either a hybrid or all-flash cluster. In hybrid clusters, flash devices are used for the cache layer and magnetic disks are used for the storage capacity layer. In all-flash clusters, flash devices are used for both cache and capacity.

You can activate vSAN on your existing host clusters and when you create clusters.

If vSAN is set to Auto mode, vSAN aggregates all free local capacity devices into a single datastore shared by all hosts in the vSAN cluster. vSAN cannot use devices that are formatted and already contain some information.

If vSAN is set to Manual mode, vSAN uses the local capacity devices that you claimed by using the vSphere Client. If you did not claim any devices through the vSphere Client, your vSAN datastore size is 0 MB.

You can expand the datastore by adding capacity devices or hosts with capacity devices to the cluster. vSAN works best when all ESXi hosts in the cluster share similar or identical configurations across all cluster members, including similar or identical storage configurations. This consistent configuration balances virtual machine storage components across all devices and hosts in the cluster. Hosts without any local devices also can participate and run their virtual machines on the vSAN datastore.

If a host contributes its local storage devices to the vSAN datastore, it must provide at least one device for flash cache and at least one device for capacity. Capacity devices are also called data disks.

The devices on the contributing host form one or more disk groups. Each disk group contains one flash cache device, and one or multiple capacity devices for persistent storage. Each host can be configured to use multiple disk groups.

For best practices, capacity considerations, and general recommendations about designing and sizing a vSAN cluster, see the *VMware vSAN Design and Sizing Guide*.

Characteristics of vSAN

This topic summarizes characteristics that apply to vSAN, its clusters, and datastores.

vSAN provides numerous benefits to your environment.

Table 4-1. vSAN Features

Supported Features	Description
Shared storage support	vSAN supports VMware features that require shared storage, such as HA, vMotion, and DRS. For example, if a host becomes overloaded, DRS can migrate virtual machines to other hosts in the cluster.
On-disk format	vSAN on-disk virtual file format provides highly scalable snapshot and clone management support per vSAN cluster. For information about the number of virtual machine snapshots and clones supported per vSAN cluster, see the *Configuration Maximums* documentation.
All-flash and hybrid configurations	vSAN can be configured for all-flash or hybrid cluster.
Fault domains	vSAN supports configuring fault domains to protect hosts from rack or chassis failures when the vSAN cluster spans across multiple racks or blade server chassis in a data center.
iSCSI target service	vSAN iSCSI target service enables hosts and physical workloads that reside outside the vSAN cluster to access the vSAN datastore.
Stretched cluster	vSAN supports stretched clusters that span across two geographic locations.
Support for Windows Server Failover Clusters (WSFC)	vSAN 6.7 Update 3 and later releases support SCSI-3 Persistent Reservations (SCSI3-PR) on a virtual disk level required by Windows Server Failover Cluster (WSFC) to arbitrate an access to a shared disk between nodes. Support of SCSI-3 PRs enables configuration of WSFC with a disk resource shared between VMs natively on vSAN datastores. Currently the following configurations are supported: ■ Up to 6 application nodes per cluster. ■ Up to 64 shared virtual disks per node. **Note** Microsoft SQL Server 2012 or later running on Microsoft Windows Server 2012 or later has been qualified on vSAN.
vSAN health service	vSAN health service includes preconfigured health check tests to monitor, troubleshoot, diagnose the cause of cluster component problems, and identify any potential risk.
vSAN performance service	vSAN performance service includes statistical charts used to monitor IOPS, throughput, latency, and congestion. You can monitor performance of a vSAN cluster, host, disk group, disk, and VMs.
Integration with vSphere storage features	vSAN integrates with vSphere data management features traditionally used with VMFS and NFS storage. These features include snapshots, linked clones, and vSphere Replication.
Virtual Machine Storage Policies	vSAN works with VM storage policies to support a VM-centric approach to storage management. If you do not assign a storage policy to the virtual machine during deployment, the vSAN Default Storage Policy is automatically assigned to the VM.

Table 4-1. vSAN Features (continued)

Supported Features	Description
Rapid provisioning	vSAN enables rapid provisioning of storage in the vCenter Server® during virtual machine creation and deployment operations.
Deduplication and compression	vSAN performs block-level deduplication and compression to save storage space. When you enable deduplication and compression on a vSAN all-flash cluster, redundant data within each disk group is reduced. Deduplication and compression is a cluster-wide setting, but the functions are applied on a disk group basis. Compression-only vSAN is applied on a per-disk basis.
Data at rest encryption	vSAN provides data at rest encryption. Data is encrypted after all other processing, such as deduplication, is performed. Data at rest encryption protects data on storage devices, in case a device is removed from the cluster.
SDK support	The VMware vSAN SDK for Java is an extension of the VMware vSphere Management SDK. It includes documentation, libraries and code examples that help developers automate installation, configuration, monitoring, and troubleshooting of vSAN.

Monitor vSAN in the VMware Host Client

You can use the VMware Host Client to monitor the vSAN environment of your ESXi host.

Prerequisites

vSAN service must be enabled in the vSphere Client before you can view the vSAN related screens for a datastore.

Procedure

1. Click **Storage** in the VMware Host Client inventory.
2. On the **Datastores** tab, click **vSAN Datastore**.

   The vSAN Datastore expands in the VMware Host Client navigator.
3. Click **Monitor**.

   You are present with the **vSAN**, **Host**, and **Health** tabs in the UI.

Option	Description
vSAN	Displays the configurations for the current host. You can edit the settings for the claiming mode and deduplication. You can also view the settings for: ■ Encryption – vSAN supports encryption of the information for the whole vSAN datastore. ■ ISCSI Service – Additional service through the iSCSI service. ■ Performance Service - Collects data on how the datastore works. For example, the speed of a read/write operation.
Hosts	Displays a list of all the hosts on the vSAN server with their IP and the fault domain they belong to.
Health	The **Health** tab contains tests organized in groups. You are present with the following groups: ■ Performance Service ■ Network ■ Physical disk ■ Data ■ Cluster ■ Limits Each group is labeled with a status icon for an error, warning, unknown or healthy. The status of the group represents the most severe state of the test belonging to that group. To view the tests and their descriptions, click the expand icon in the top right corner of the group of interest. From the expanded card you can review all the tests belonging to the group, the result of their execution and get more information about what each test examines on the system.

4 Select the vSAN parameter that you want to monitor.

Edit Settings for a vSAN Datastore

You can edit the settings for a vSAN datastore when you must exit from a misconfigured state of the current host.

You can only edit the **Claiming Mode** and **Deduplication** settings for a vSAN datastore. These changes take effect only on the current host. They are not synced to the other hosts participating into the vSAN cluster.

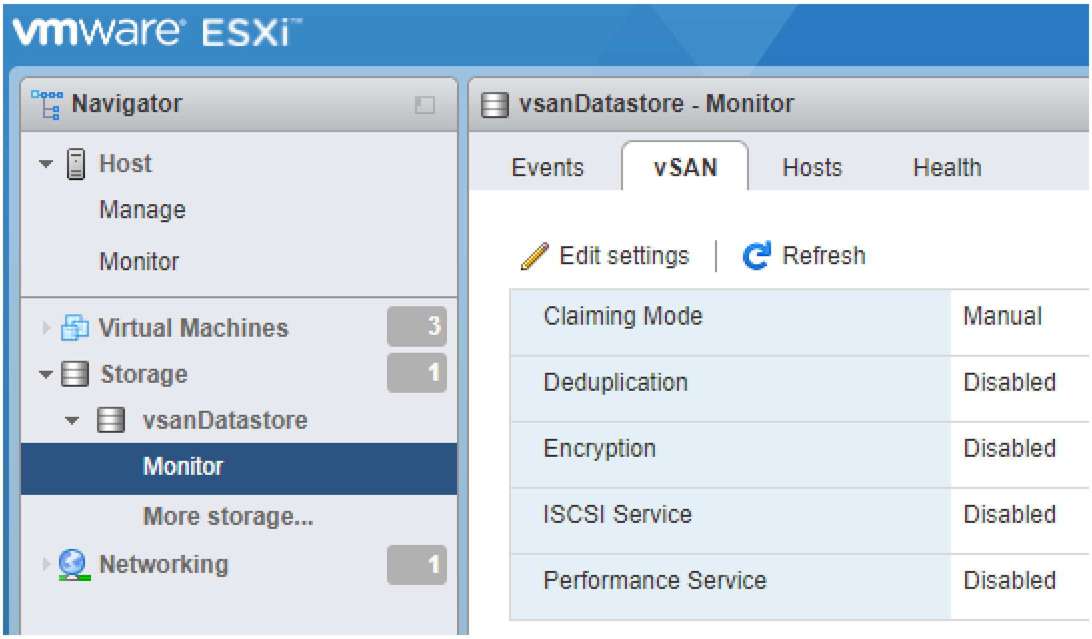
Note Only use these settings for troubleshooting.

Procedure

1 Click **Storage** in the VMware Host Client inventory.

2 On the **Datastores** tab, click a vSAN datastore from the table.

3 Click **Monitor** and click the **vSAN** tab.



Claiming Mode	Manual
Deduplication	Disabled
Encryption	Disabled
ISCSI Service	Disabled
Performance Service	Disabled

4 Click **Edit settings**.

The **Edit Settings** dialog box opens.

5 Change the settings.Select **Auto** or **Manual** from the **Claiming Mode**.

Option	Action
Claiming Mode	a Select **Auto** or **Manual** from the **Claiming Mode**. ■ If you select **Auto**, it automatically takes all disks and claims them in a group or groups of the same size. **Note** The **Auto** mode is deprecated. It can only claim hybrid disk groups which are not compatible with most of the vSAN features. ■ If you select **Manual**, you must manually organize the disks in groups and reclaim them by using the vSphere Web Client. For instance, selecting manual claiming mode is appropriate when the vCenter Server is unavailable.
Deduplication	a Select **Enabled** or **Disabled** for the **Deduplication**.

6 Click **Save**.

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

The range of scanned LUN IDs for an ESXi host can be from 0 to 16,383. ESXi ignores LUN IDs greater than 16,383. The configurable `Disk.MaxLUN` parameter controls the range of scanned LUN ID range. The parameter has a default value of 1024.

The `Disk.MaxLUN` parameter also determines how many LUNs the SCSI scan code attempts to discover using individual INQUIRY commands if the SCSI target does not support direct discovery 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 1 through 100, set the value to 101. As a result, you can 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 also depend on other factors, including the type of the 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:

Managing Port Groups in the VMware Host Client

You can manage port group settings to configure traffic management, enhance networking security, and enhance performance. By using the VMware Host Client, you can add and remove port groups. You can also examine port group information and edit port group settings, such as NIC teaming and traffic shaping.

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 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 Switch Port Group in the VMware Host Client

You can add a port group to a virtual switch in the VMware Host Client. 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 pop-up 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 Expand **Security** and select options that you want to enable for promiscuous mode, MAC address changes, and forged transmits.

6 Click **Add**.

   Your port group is created.

7 (Optional) Click **Refresh** to display the new port group in the list.

Edit Port Group Settings in the VMware Host Client

To enhance networking security and improve networking performance in the VMware Host Client, you can edit various port group settings, such as the port group name, VLAN ID, and virtual switch. You can also configure security, NIC teaming, and traffic shaping components.

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 port group name.

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 (Optional) Expand **Security** and select whether to reject, accept, or inherit the Security policy exceptions from vSwitch.

Option	Description
Promiscuous Mode	■ **Reject**. Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter. ■ **Accept**. Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the vSphere distributed switch that are allowed under the VLAN policy for the port group that the adapter is connected to. ■ **Inherit from vSwitch**. Placing a guest adapter in promiscuous mode causes it to inherit the configuration from the associated virtual switch.
MAC Address Changes	■ **Reject**. If you set the **MAC Address Changes** to **Reject** and the guest operating system changes the MAC address of the adapter to anything other than what is in the `.vmx` configuration file, all inbound frames are dropped. If the guest operating system changes back the MAC address to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. ■ **Accept**. Changing the MAC address from the guest operating system has the intended effect: frames to the new MAC address are received. ■ **Inherit from vSwitch**. If you set **MAC Address Changes** to **Inherit from vSwitch**, the MAC address changes to one of the associated virtual switches.
Forged Transmits	■ **Reject**. Any outbound frame with a source MAC address that is different from the one set on the adapter are dropped. ■ **Accept**. No filtering is performed and all outbound frames are passed. ■ **Inherit from vSwitch**. The outbound frame configuration is inherited from the associated virtual switch.

7 (Optional) Expand **NIC teaming** and configure the following components.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Inherit from vSwitch**. Choose the uplink that is selected for the associated virtual switch. ■ **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash. ■ **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet. ■ **Route based on originating port ID**. Choose an uplink based on the originating port ID. ■ **Use explicit failover order**. Always use the highest order uplink from the list of active adapters which passes failover detection criteria . **Note** IP-based teaming requires the physical switch to be configured with EtherChannel. For all other options, EtherChannel must be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ ■ **Inherit from vSwitch**. Inherits the respective configuration of the associated virtual switch. ■ **Link Status only**. Relies only on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by a spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. ■ **Beacon only**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine a link failure. This detects many of the failures that are not detected by link status only. **Note** Do not use beacon probing with IP-hash load balancing.
Notify Switches	Select **Yes**, **No**, or **Inherit from vSwitch** to notify switches if a failover occurs. If you select **Yes**, when a virtual NIC is connected to the distributed switch or that virtual NIC's traffic is routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this process is preferred for the lowest latency of failover occurrences and migrations with vMotion. **Note** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.

Option	Description
Failback	Select **Yes**, **No**, or **Inherit from vSwitch** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to the default setting of **Yes**, the adapter returns to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to **No**, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Failover Order	Specify how to distribute the workload for uplinks. If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, set this condition by moving them into different groups: ■ **Active Uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. ■ **Standby Uplinks** . Use this uplink if one of the active adapter's connectivities is down. **Note** When using IP-hash load balancing, do not configure standby uplinks. You cannot configure failover order if any of the port group components are configured to inherit the configuration from the associated virtual switch.

8 (Optional) To configure traffic shaping, expand **Traffic shaping**, click **Enabled**, and specify the following parameters.

Option	Description
Average Bandwidth	Establishes the number of bits per second to limit across a port, averaged over time—the allowed average load.
Peak Bandwidth	The maximum number of bits per second to limit across a port when it is sending/receiving a burst of traffic. This is the maximum bandwidth used by a port whenever it is using its burst bonus.
Burst Size	The maximum number of bytes to limit in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average Bandwidth**, it might be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter represents the maximum number of bytes that might be accumulated in the burst bonus and so transferred at a higher speed.

Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.

9 Click **Save** to apply your changes.

Remove a Virtual Switch 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 the **Port groups** tab.

2 Right-click the port group that you want to remove and select **Remove** from the pop-up menu.

3 To remove the port group, click **Remove**.

4 (Optional) Click **Refresh** to verify that you have removed the port group.

Managing Virtual Switches in the VMware Host Client

In the VMware Host Client, you can configure various virtual switch settings, such as link discovery, NIC teaming, and traffic shaping.

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, and to handle VMkernel traffic. Depending on the type of connection that you want to create, you can create 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 Expand **Link discovery** and select an option for the virtual switch mode.

Operation	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere Standard Switch is not available to the switch administrator.
Advertise	ESXi makes information about the vSphere Standard Switch available to the switch administrator, but does not detect and display information about the physical switch.
Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere Standard Switch available to the switch administrator.
None	ESXi does not detect or display information about the associated physical switch port, and information about the vSphere Standard Switch is not available to the switch administrator.

6 In the Protocol section, select **Cisco Discovery Protocol** from the drop-down menu.

7 Expand **Security** and accept or reject promiscuous mode, MAC address changes, and forged transmits of the virtual machines attached to the standard switch.

Option	Description
Promiscuous mode	■ **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. ■ **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	■ **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. ■ **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	■ **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. ■ **Accept**. The switch does not perform filtering, and permits all outbound frames.

8 Click **Add**.

Remove a Standard Virtual Switch in the VMware Host Client

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

Procedure

1 Click **Networking** in the VMware Host Client inventory and click the **Virtual switches** tab.

2 Right-click the virtual switch that you want to remove from the list and click **Remove**.

3 Click **Yes**.

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 virtual switch settings, such as 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 Change the maximum transmission unit (MTU).

   The MTU improves the networking efficiency by increasing the amount of payload data transmitted with a single packet, that is, enabling jumbo frames.

5 (Optional) Click the **Remove** icon (⊗) to remove the old uplink from the virtual switch.

6 Expand **Link discovery** and select an option for the virtual switch mode.

Operation	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere Standard Switch is not available to the switch administrator.
Advertise	ESXi makes information about the vSphere Standard Switch available to the switch administrator, but does not detect and display information about the physical switch.

Operation	Description
Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere Standard Switch available to the switch administrator.
None	ESXi does not detect or display information about the associated physical switch port, and information about the vSphere Standard Switch is not available to the switch administrator.

7 In the Protocol section, select **Cisco Discovery Protocol** from the drop-down menu.

8 Expand **Security** and accept or reject promiscuous mode, MAC address changes, and forged transmits of the virtual machines attached to the standard switch.

Option	Description
Promiscuous mode	■ **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. ■ **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	■ **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. ■ **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	■ **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. ■ **Accept**. The switch does not perform filtering, and permits all outbound frames.

9 (Optional) Expand **NIC teaming** and configure the following components.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash. ■ **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet. ■ **Route based on originating port ID**. Choose an uplink based on the originating port ID. ■ **Use explicit failover order**. Always use the highest order uplink from the list of Active adapters which passes failover detection criteria. **Note** IP-based teaming requires the physical switch to be configured with EtherChannel. For all other options, EtherChannel must be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ **Link Status only**. Relies only on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. ■ **Beacon only**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This detects many of the failures previously mentioned that are not detected by link status alone. **Note** Do not use beacon probing with IP-hash load balancing.
Notify Switches	Select **Yes**, **No**, or **Inherit from vSwitch** to notify switches in the case of failover. If you select **Yes**, whenever a virtual NIC is connected to the distributed switch or whenever that virtual NIC's traffic might be routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this process is desirable for the lowest latency of failover occurrences and migrations with vMotion. **Note** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.

Option	Description
Failback	Select **Yes**, **No**, or **Inherit from vSwitch** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to **Yes** (default), the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to **No**, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Failover Order	Specify how to distribute the work load for uplinks. If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, set this condition by moving them into different groups: ■ **Active Uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. ■ **Standby Uplinks** . Use this uplink if one of the active adapter's connectivities is down. **Note** When using IP-hash load balancing, do not configure standby uplinks.

10 (Optional) To configure traffic shaping, expand **Traffic shaping**, click **Enabled**, and specify the following parameters.

Option	Description
Average Bandwidth	Establishes the number of bits per second to allow across a port, averaged over time—the allowed average load.
Peak Bandwidth	The maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This tops the bandwidth used by a port whenever it is using its burst bonus.
Burst Size	The maximum number of bytes to allow in a burst. If this parameter is set, a port may gain a burst bonus when it doesn't use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average Bandwidth**, it may be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that may be accumulated in the burst bonus and then transferred at a higher speed.

Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.

11 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 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 VMware vSphere® Standard Edition™ switch to provide network connectivity for hosts. The VMkernel NIC also handles the system traffic for VMware vSphere® vMotion®, IP storage, Fault Tolerance, logging, vSAN, and so on.

Procedure

1 Right-click **Networking** in the VMware Host Client inventory and click **Add VMkernel NIC**.

2 In the **Add VMkernel NIC** dialog box, configure the settings for the VMkernel adapter.

Option	Description
New port group Label	Adding a VMkernel NIC also adds a 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 Select a virtual switch from the drop-down menu.

4 (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.

5 (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	a Click **Add address** to add a new IPv6 address. b Enter the IPv6 address and subnet prefix length.

6 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. Such operations include traffic Provisioning, such as virtual machine cold migration, cloning, and snapshot migration.

7 (Optional) Select the services to enable 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. You cannot 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 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

1 Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.

2 Select the VMkernel adapter that resides on the target standard switch, click **Actions**, and select **Edit settings** from the drop-down menu.

3 (Optional) Edit the VLAN ID.

   The VLAN ID determines the VLAN that the network traffic of the VMkernel adapter uses.

4 (Optional) To edit the IP version, select IPv4, IPv6, or both from the drop-down menu.

   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 a router advertisement to obtain IPv6 addresses.
Static IPv6 Addresses	a Click **Add address** to add an IPv6 address. b Enter the IPv6 address and subnet prefix length.

7 (Optional) Select the service to enable or disable 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 the 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.