vSphere Administration with the vSphere Client

vCenter Server 6.0
ESXi 6.0

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

EN-001606-02

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2015 VMware, Inc. All rights reserved. Copyright and trademark information.

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

Contents

vSphere Administration with the vSphere Client 9

Updated Information 11

1 Using the vSphere Client 13
- Start the vSphere Client and Log In 14
- Stop the vSphere Client and Log Out 14
- Status Bar and Recent Tasks 14
- Getting Started Tabs 15
- View Virtual Machine Console 15
- Using Lists 16
- Save vSphere Client Data 17
- Panel Sections 17
- Searching the vSphere Inventory 17
- Custom Attributes 18
- Select Objects 20
- Manage vCenter Server Plug-Ins 20
- Working with Active Sessions 21

2 Configuring ESXi Hosts and vCenter Server in the vSphere Client 23
- Configuring ESXi Hosts 23
- Configuring vCenter Server in the vSphere Client 26
- Configuring Communication Among ESXi , vCenter Server, and the vSphere Client 32
- Reboot or Shut Down an ESXi Host 32

3 Organizing Your Inventory 35
- Create Datacenters 36
- Add Hosts 37
- Create Clusters 38
- Create Resource Pools 38
- Create Datastores 39
- Create Host-Wide Networks 40
- Create Datacenter-Wide Networks 40

4 Managing License Keys in the vSphere Client 45
- Licensing Limitations in the vSphere Client 45
- Managing License Keys on ESXi Hosts 45
- Managing License Keys on vCenter Server 47

5 Managing Tasks 51
- Viewing Tasks 51

Cancel a Task 53
Schedule Tasks 53
Policy Rules for Task Operations 57

6 Securing the Management Interface 59
Securing ESXi Hosts 59
Securing Virtual Machines 63

7 ESXi Authentication and User Management 69
Managing Users with the vSphere Client 69
Assigning Permissions for ESXi 72
Managing ESXi Roles 73
Using Active Directory to Manage ESXi Users 76
Use vSphere Authentication Proxy to Add a Host to a Domain 77
Adjust the Search List in Large Domains 78

8 Managing Hosts in vCenter Server 79
Disconnecting and Reconnecting a Host 79
Remove a Host from a Cluster 80
Remove a Managed Host from vCenter Server 81

9 Using vCenter Maps 83
Set the Maximum Number of Map Objects 84
View vCenter Maps 84
Print vCenter Maps 84
Export vCenter Maps 84

10 Creating a Virtual Machine in the vSphere Client 85
Start the Virtual Machine Creation Process in the vSphere Client 85
Select a Configuration Option for the New Virtual Machine in the vSphere Client 86
Enter a Name and Location for the Virtual Machine in the vSphere Client 87
Select a Host or Cluster in the vSphere Client 87
Select a Resource Pool in the vSphere Client 88
Select a Datastore in the vSphere Client 88
Select a Virtual Machine Version in the vSphere Client 89
Select an Operating System in the vSphere Client 89
Select the Number of Virtual CPUs in the vSphere Client 90
Configure Virtual Memory in the vSphere Client 90
Configure Networks in the vSphere Client 91
Select a SCSI Controller in the vSphere Client 92
Selecting a Virtual Disk Type 92
Complete Virtual Machine Creation in the vSphere Client 96

11 Working with Templates and Clones in the vSphere Client 97
Clone a Virtual Machine in the vSphere Client 97
Create a Scheduled Task to Clone a Virtual Machine in the vSphere Client 100
Create a Template in the vSphere Client 100
Deploy a Virtual Machine from a Template in the vSphere Client 103

Change Template Name in the vSphere Client 105
Deleting Templates 106
Convert a Template to a Virtual Machine in the vSphere Client 107

12 Customizing Guest Operating Systems 109
Guest Operating System Customization Requirements 109
Configure a Script to Generate Computer Names and IP Addresses During Guest Operating System Customization in the vSphere Client 110
Customize Windows During Cloning or Deployment in the vSphere Client 111
Customize Linux During Cloning or Deployment in the vSphere Client 113
Managing Customization Specifications in the vSphere Client 115

13 Migrating Virtual Machines in the vSphere Client 123
Migrate a Powered-On Virtual Machine with vMotion in the vSphere Client 124
Migrate a Virtual Machine with Storage vMotion in the vSphere Client 125
Migrate a Powered-Off or Suspended Virtual Machine in the vSphere Client 126
CPU Compatibility and EVC 128

14 Deploying OVF Templates 133
Deploy an OVF Template in the vSphere Client 133
Export an OVF Template 134

15 Configuring Virtual Machines in the vSphere Client 137
Virtual Machine Limitations in the vSphere Client 138
Virtual Machine Hardware Versions 139
Locate the Hardware Version of a Virtual Machine in the vSphere Client 140
Change the Virtual Machine Name in the vSphere Client 141
View the Virtual Machine Configuration File Location in the vSphere Client 141
Edit Configuration File Parameters in the vSphere Client 141
Change the Configured Guest Operating System in the vSphere Client 142
Configure Virtual Machines to Automatically Upgrade VMware Tools 142
Virtual CPU Configuration 143
Virtual Memory Configuration 149
Network Virtual Machine Configuration 153
Parallel and Serial Port Configuration 154
Virtual Disk Configuration 160
SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility 163
Other Virtual Machine Device Configuration 167
Configuring vServices 172
USB Configuration from an ESXi Host to a Virtual Machine 173
USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client 177
Manage Power Management Settings for a Virtual Machine 180
Configure the Virtual Machine Power States 180
Delay the Boot Sequence in the vSphere Client 182
Enable Logging in the vSphere Client 182
Disable Acceleration in the vSphere Client 183
Configure Debugging and Statistics in the vSphere Client 183

16 Managing Virtual Machines 185
Edit Virtual Machine Startup and Shutdown Settings 185
Open a Console to a Virtual Machine 186
Adding and Removing Virtual Machines 186
Using Snapshots To Manage Virtual Machines 187

17 Managing Multi-Tiered Applications with vSphere vApp in the vSphere Client 195
Create a vApp 196
Power On a vApp in the vSphere Client 197
Clone a vApp 198
Power Off a vApp in the vSphere Client 198
Suspend a vApp in the vSphere Client 198
Resume a vApp in the vSphere Client 199
Populate the vApp 199
Edit vApp Settings in the vSphere Client 200
Configuring IP Pools 204
Edit vApp Annotation in the vSphere Client 206

18 Monitoring Solutions with the vCenter Solutions Manager 207
Viewing Solutions 208
Monitoring Agents 208
Monitoring vServices 209

19 Using Host Profiles in the vSphere Client 211
Host Profiles Usage Model 211
Access Host Profiles View 212
Creating a Host Profile 212
Export a Host Profile 213
Import a Host Profile 214
Clone a Host Profile 214
Edit a Host Profile 214
Manage Profiles 217
Checking Compliance 220
Host Profiles and vSphere Auto Deploy 222

20 Networking in the vSphere Client 225
Networking Limitations in the vSphere Client 225
View Networking Information in the vSphere Client 226
View Network Adapter Information in the vSphere Client 226
Setting Up Networking with vSphere Standard Switches 227
Setting Up Networking with vSphere Distributed Switches 230

21 Managing Network Resources 247
vSphere Network I/O Control 247
TCP Segmentation Offload and Jumbo Frames 250
DirectPath I/O 252
Single Root I/O Virtualization (SR-IOV) 254

22 Networking Policies 257
Applying Networking Policies on a vSphere Standard or Distributed Switch 257
Teaming and Failover Policy 259
VLAN Policy 267
Security Policy 269
Traffic Shaping Policy 273
Resource Allocation Policy 277
Monitoring Policy 278
Port Blocking Policies 279
Manage Policies for Multiple Port Groups on a vSphere Distributed Switch 279

23 Advanced Networking 285
Internet Protocol Version 6 (IPv6) Support 285
VLAN Configuration 286
Working With Port Mirroring 286
Configure NetFlow Settings 293
Switch Discovery Protocol 293
Change the DNS and Routing Configuration 295
MAC Address Management 296

24 Managing Storage in the vSphere Client 299
Storage Limitations in the vSphere Client 300
Display Storage Devices for a Host in the vSphere Client 300
Display Storage Devices for an Adapter in the vSphere Client 301
View Storage Adapters Information in the vSphere Client 301
Review Datastore Information in the vSphere Client 301
Assign WWNs to Virtual Machines 301
Modify WWN Assignments 302
Set Up Networking for Software FCoE 303
Add Software FCoE Adapters 304
Disable Automatic Host Registration 304
Setting Up Independent Hardware iSCSI Adapters 305
Configuring Dependent Hardware iSCSI Adapters 306
Configuring Software iSCSI Adapters 308
Setting Up iSCSI Network 310
Using Jumbo Frames with iSCSI 315
Configuring Discovery Addresses for iSCSI Adapters 316
Configuring CHAP Parameters for iSCSI Adapters 317
Configure Advanced Parameters for iSCSI in the vSphere Client 320
Managing Storage Devices 321
Working with Datastores 322
Raw Device Mapping 332
Understanding Multipathing and Failover 333
Storage Hardware Acceleration 335
Storage Thin Provisioning 336
Using Storage Vendor Providers 338

25 Resource Management for Single Hosts 341
Configuring Resource Allocation Settings 341
Administering CPU Resources 342
Administering Memory Resources 345
Managing Storage I/O Resources 349
Managing Resource Pools 352
Using DRS Clusters to Manage Resources 356
Creating a Datastore Cluster 368
Using Datastore Clusters to Manage Storage Resources 371
Using NUMA Systems with ESXi 379
Advanced Attributes 381

26 Creating and Using vSphere HA Clusters 383
vSphere HA Checklist 383
Creating and Configuring a vSphere HA Cluster 384
Customize an Individual Virtual Machine in the vSphere Client 389

27 Providing Fault Tolerance for Virtual Machines 391
Fault Tolerance Use Cases 391
Fault Tolerance Checklist 392
Preparing Your Cluster and Hosts for Fault Tolerance 393
Using Fault Tolerance 396
Viewing Information About Fault Tolerant Virtual Machines in the vSphere Client 398
Best Practices for Fault Tolerance 400

28 Monitoring a Single Host with the vSphere Client 403
View Charts 403
Working with Advanced and Custom Charts 403
Monitoring Host Health Status 406
Monitoring Events, Alarms, and Automated Actions 408
Viewing Solutions 422
Configure SNMP Settings for vCenter Server 423
System Log Files 424

Index 429

vSphere Administration with the vSphere Client

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

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

Intended Audience

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

Updated Information

This *vSphere Administration with the vSphere Client* is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Administration with the vSphere Client* .

Revision	Description
EN-001606-02	Removed information related to vSphere Storage Appliance. This functionality is deprecated in vSphere 6.0.
EN-001606-01	■ Removed information related to Storage Views and Storage Reports. This functionality is deprecated inv Sphere 6.0. ■ Updated the number of LUN IDs in "Change the Number of Scanned Storage Devices," on page 322 ■ Added licensing limitation topic "Licensing Limitations in the vSphere Client," on page 45.
EN-001606-00	Initial release.

Using the vSphere Client 1

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

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

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

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

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

This chapter includes the following topics:

- "Start the vSphere Client and Log In," on page 14
- "Stop the vSphere Client and Log Out," on page 14
- "Status Bar and Recent Tasks," on page 14
- "Getting Started Tabs," on page 15
- "View Virtual Machine Console," on page 15
- "Using Lists," on page 16
- "Save vSphere Client Data," on page 17
- "Panel Sections," on page 17
- "Searching the vSphere Inventory," on page 17
- "Custom Attributes," on page 18
- "Select Objects," on page 20
- "Manage vCenter Server Plug-Ins," on page 20
- "Working with Active Sessions," on page 21

Start the vSphere Client and Log In

The vSphere Client is a graphical user interface for ESXi host and vCenter Server management.

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

Procedure

1 Log in to your Windows system.

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

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

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

3 Enter the IP address or server name, your user name, and your password.

4 Click **Login** to continue.

You are now connected to the host.

NOTE If you connect to an ESXi host that is currently managed by a vCenter Server system, you will receive a warning message and changes made to the host may not be reflected in the vCenter Server system

---

Stop the vSphere Client and Log Out

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

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

Procedure

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

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

Status Bar and Recent Tasks

Use the status bar to view information about recently completed or active tasks.

The status bar appears at the bottom of the window. It displays any currently running or recently completed active tasks. Included is a progress bar indicating the percentage complete of each task.

Getting Started Tabs

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

- Disable Getting Started Tabs on page 15

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

- Restore Getting Started Tabs on page 15

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

Disable Getting Started Tabs

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

You can disable the tabs in the following ways.

Procedure

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

Restore Getting Started Tabs

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

Procedure

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

View Virtual Machine Console

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

Procedure

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

Using Lists

Many vSphere Client inventory tabs display lists of information.

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

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

Filter a List View

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

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

Procedure

1 On any inventory panel that displays a list, click the arrow next to the filter box at the top right of the pane.

2 Select the attributes on which to filter.

3 Enter search criteria into the filter field.

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

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

Export a List

You can export a list in the vSphere Client to a file. Multiple file types are available when saving the file locally.

Procedure

1 In the vSphere Client, navigate to a list view. For example, click the **Virtual Machines** tab when viewing a host.

2 Select **File > Export > Export List**.

3 Type a filename and select a file type.

4 Click **Save**.

Save vSphere Client Data

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

Procedure

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

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

Panel Sections

The body of the vSphere Client page has a panel section. Most views have a left and a right panel: the Inventory panel and the Information panel.

You can resize these panels.

Inventory panel	Displays a hierarchical list of vSphere objects when an Inventory or Maps view appears.
Information panels	Display lists and charts. Depending on the navigation items or Inventory item selected, the Information panel is divided into tabbed elements.

Searching the vSphere Inventory

When you are connected to a vCenter Server system with the vSphere Client, you can search the vSphere inventory for virtual machines, hosts, datastores, networks, or folders that match specified criteria.

If the vSphere Client is connected to a vCenter Server system that is part of a connected group in vCenter Linked Mode, you can search the inventories of all vCenter Server systems in that group. You can view and search only for inventory objects that you have permission to view. Because the search service queries Active Directory for information about user permissions, you must be logged in to a domain account to search all vCenter Server systems in Linked Mode. If you log in using a local account, searches return results only for the local vCenter Server system, even if it is joined to other servers in Linked Mode.

NOTE If your permissions change while you are logged in, the search service might not immediately recognize these changes. To ensure that your search is performed with up-to-date permissions, log out of all your open sessions and log in again before performing the search.

Perform a Simple Search

A simple search searches all the properties of the specified type or types of objects for the entered search term.

Procedure

1 Click the icon in the search field at the top right of the vSphere Client window and select the type of inventory item to search for.

- **Virtual Machines**
- **Hosts**

- **Folders**
- **Datastores**
- **Networks**
- **Inventory**, which finds matches to the search criteria in any of the available managed object types.

2 Type one or more search terms into the search field and press Enter.

3 (Optional) If more items are found than can be displayed in the results pane, click **Show all**.

What to do next

If you are not satisfied with the results of the simple search, perform an advanced search.

Perform an Advanced Search

Using advanced search allows you to search for managed objects that meet multiple criteria. For example, you can search for virtual machines matching a particular search string which reside on hosts whose names match a second search string.

Prerequisites

- Open a vSphere Client session to a vCenter Server system

Procedure

1 In the vSphere Client, select **View > Inventory > Search** to display the advanced search page.

2 Click the icon in the search text box and select the type of object you want to search for.

3 Type one or more search terms into the search text box.

4 (Optional) Refine the search based on additional properties.

   a Click **Show options**.

   b From the drop-down menu, select the additional property that you want to use to restrict the search results. The available properties depend on the type of object you are searching for.

   c Select or type the appropriate options for the property you have selected.

   d To add more properties, click **Add** and repeat steps a through c.

   An advanced search always finds objects that match all the properties in the list.

5 Click **Search**.

   The search results are displayed below the search specification.

Custom Attributes

You can use custom attributes to associate user-specific meta-information with virtual machines and managed hosts.

Attributes are the resources that are monitored and managed for all the managed hosts and virtual machines in your vSphere environment. Attributes' status and states appear on the inventory panels.

After you create the attributes, set the value for the attribute on each virtual machine or managed host, as appropriate. This value is stored with vCenter Server and not with the virtual machine or managed host. Use the new attribute to filter information about your virtual machines and managed hosts. If you no longer need the custom attribute, remove it. A custom attribute is always a string.

For example, suppose you have a set of products and you want to sort them by sales representative. Create a custom attribute for sales person name, Name. Add the custom attribute, Name, column to one of the list views. Add the appropriate name to each product entry. Click the column title Name to sort alphabetically.

The custom attributes feature is available only when you are connected to a vCenter Server system.

- Add Custom Attributes on page 19

  You can create custom attributes to associate with virtual machines or managed hosts.

- Edit a Custom Attribute on page 19

  You can edit custom attributes and add annotations for a virtual machine or host from the Summary tab for the object. Annotations can be used to provide additional descriptive text or comments for an object.

Add Custom Attributes

You can create custom attributes to associate with virtual machines or managed hosts.

Procedure

1 Select **Administration > Custom Attributes**.

  This option is not available when connected only to an ESXi host.

2 Click **Add**.

3 Enter the values for the custom attribute.

  a Type the name of the attribute in the **Name** text box.

  b Select the attribute type from the **Type** drop-down menu: **Virtual Machine**, **Host**, or **Global**.

  c In the **Value** text box, type the value you want to give to the attribute for the currently selected object.

  d Click **OK**.

  After you have defined an attribute on a single virtual machine or host, it is available to all objects of that type in the inventory. However, the value you specify is applied only to the currently selected object.

4 (Optional) To change the attribute name, click in the **Name** field and type the name you want to assign to the attribute.

5 Click **OK**.

Edit a Custom Attribute

You can edit custom attributes and add annotations for a virtual machine or host from the Summary tab for the object. Annotations can be used to provide additional descriptive text or comments for an object.

Procedure

1 Select the virtual machine or host in the inventory.

2 Click the **Summary** tab for the virtual machine or host.

3 In the Annotations box, click the **Edit** link.

  The Edit Custom Attributes dialog box appears.

4 To edit the value of an attribute that has already been defined, double-click the **Value** field for that attribute and enter the new value.

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

Select Objects

vCenter Server objects are datacenters, networks, datastores, resource pools, clusters, hosts, and virtual machines. Selecting an object allows you to view the status of the object and enables the menus so you can select actions to take on the object.

Procedure

- Locate the object by browsing or search.
  - From the vSphere Client Home page, click the icon for the appropriate inventory view, and browse through the inventory hierarchy to select the object.
  - Perform a search for the object, and double-click it in the search results.

Manage vCenter Server Plug-Ins

After the server component of a plug-in is installed and registered with vCenter Server, its client component is available to vSphere clients. Client component installation and enablement are managed through the Plug-in Manager dialog box.

The Plug-in Manager lets you perform the following actions:

- View available plug-ins that are not currently installed on the client.
- View installed plug-ins.
- Download and install available plug-ins.
- Enable and disable installed plug-ins.

Install Plug-Ins

You can install plug-ins using the Plug-in Manager.

Procedure

1. Launch the vSphere Client and log in to a vCenter Server system.
2. Select **Plug-ins > Manage Plug-ins**.
3. Select the **Available Plug-ins** tab in the Plug-in Manager dialog box.
4. Click **Download and Install** for the plug-in you want.
5. Follow the prompts in the installation wizard.
6. After installation is complete, verify that the plug-in is listed under the **Installed Plug-ins** tab and that it is enabled.

   There might be short delay between the completion of the installation and the plug-in appearing in the list of installed plug-ins.

Disable and Enable Plug-Ins

You can disable or enable plug-ins using the Plug-in Manager.

Disabling a plug-in does not remove it from the client. You must uninstall the plug-in to remove it.

Procedure

1. Launch the vSphere Client and log in to a vCenter Server system.
2. Select **Plug-ins > Manage Plug-ins**.

3 Select the **Installed** tab in the Plug-in Manager dialog box.

4 Right-click on a plug-in and select **Enable** to enable a plug-in, or select **Disable** to disable it.

Remove Plug-Ins

You can remove plug-ins through the operating system's control panel.

Procedure

- Consult your operating system's documentation for instructions on how to use the Add/Remove Programs control panel.

Troubleshooting vCenter Server Plug-Ins

In cases where vCenter Server plug-ins are not working, you have several options to correct the problem.

vCenter Server plug-ins that run on the Tomcat server have `extension.xml` files, which contain the URL where the corresponding Web application can be accessed. These files are located in `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions`. Extension installers populate these XML files using the DNS name for the machine.

Example from the stats `extension.xml` file: `<url>https://SPULOV-XP-VM12.vmware.com:8443/statsreport/vicr.do</url>`.

vCenter Server, plug-in servers, and the clients that use them must be located on systems under the same domain. If they are not under the same domain, or if the DNS of the plug-in server is changed, the plug-in clients will not be able to access the URL, and the plug-in will not work.

You can edit the XML files manually by replacing the DNS name with an IP address. Reregister the plug-in after you edit its `extension.xml` file.

Working with Active Sessions

You can view a list of users who are logged in to a vCenter Server system when your vSphere Client is connected to that server. You can end sessions, and you can send a message to all users logged on to an active session.

These features are not available when your vSphere Client is connected to an ESXi host.

View Active Sessions

You can view active sessions on the home page of a vSphere Client.

Procedure

- From the Home page of a vSphere Client connected to a vCenter Server system, click the **Sessions** button.

Terminate Active Sessions

Terminating an active session ends the vSphere Client session and any remote console connections started by the user during the session.

Procedure

1 On the Home page of a vSphere Client connected to a vCenter Server system, click the **Sessions** button.

2 Right-click a session and select **Terminate Session**.

3 Click **OK** to confirm the termination.

Send a Message to All Active Users

You can send a Message of the Day to all active session users and to new users when they log into the vSphere Client.

The **Message of the day** text is sent as a notice message to all active session users and to new users when they log in.

Procedure

1 On the Home page of a vSphere Client connected to a vCenter Server system, click the **Sessions** button.

2 Type a message in the **Message of the day** field.

3 Click **Change**.

The message is broadcast to all users logged into the vSphere Client.

Configuring ESXi Hosts and vCenter Server in the vSphere Client 2

Use the vSphere Client to configure ESXi and vCenter Server settings.

This chapter includes the following topics:

- "Configuring ESXi Hosts," on page 23
- "Configuring vCenter Server in the vSphere Client," on page 26
- "Configuring Communication Among ESXi, vCenter Server, and the vSphere Client," on page 32
- "Reboot or Shut Down an ESXi Host," on page 32

Configuring ESXi Hosts

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

Host Limitations in the vSphere Client

The host configuration tasks that you can perform when you connect directly to an ESXi host or vCenter Server system with the vSphere Client are limited.

The following host features are unavailable or read-only in the vSphere Client

- Deleted file reclamation
- Guest authorization
- Host profiles reference host independence
- Lockdown mode

Use the vSphere Web Client as the primary interface for managing the full range of host functions available in your vSphere 6.0 environment.

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

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

Prerequisites

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

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

Procedure

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

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

Set the Scratch Partition in the vSphere Client

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

Prerequisites

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

Procedure

1. In the vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.
3. Under Software, click **Advanced Settings**.
4. Select **ScratchConfig**.

   The field **ScratchConfig.CurrentScratchLocation** shows the current location of the scratch partition.
5. In the field **ScratchConfig.ConfiguredScratchLocation**, enter a directory path that is unique for this host.
6. Reboot the host for the changes to take effect.

Configure Syslog on ESXi Hosts

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

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

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

Procedure

1. In the vSphere Client inventory, select the host.
2. Click the **Configuration** tab.
3. In the Software panel, click **Advanced Settings**.

4 Select **Syslog** in the tree control.

5 To set up logging globally, click **global** and make changes to the fields on the right.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified 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.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

6 (Optional) To overwrite the default log size and log rotation for any of the logs.

   a Click **loggers**.

   b Click the name of the log you that want to customize and enter the number of rotations and log size you want.

7 Click **OK**.

Changes to the syslog options take effect immediately.

Set the Host Image Profile Acceptance Level

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

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

Prerequisites

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

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Under Software, click **Security Profile**.

3 Under Host Image Profile Acceptance Level, click **Edit**.

4 Select the acceptance level and click **OK**.

Table 2-1. Host Image Profile Acceptance Levels

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMware Certified	VMware Certified
VMware Accepted	VMware Certified, VMware Accepted
Partner Supported	VMware Certified, VMware Accepted, Partner Supported
Community Supported	VMware Certified, VMware Accepted, Partner Supported, Community Supported

Configuring vCenter Server in the vSphere Client

Use the vCenter Server Settings dialog box to configure licensing, statistics collection, logging and other settings.

vCenter Server Limitations in the vSphere Client

The vCenter Server tasks that you can perform when you connect directly to vCenter Server with the vSphere Client are limited.

The following vCenter Server features are unavailable or read-only in the vSphere Client:

- Runtime settings
- Licensing reports
- Certificate management
- Creating and managing categories and tags

Use the vSphere Web Client as the primary interface for managing the full range of vCenter Server functions available in your vSphere 6.0 environment.

Configure License Settings for vCenter Server

You must configure a license to use vCenter Server. License keys are required for various vSphere components and features.

Prerequisites

To configure licenses, the vSphere Client must be connected to a vCenter Server system.

Required privilege: **Global.Settings**

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 If the vCenter Server system is part of a connected group, select the server you want to configure from the **Current vCenter Server** drop-down menu.

3 In the **vCenter License** section, select the type of license key to assign to this vCenter Server.

- Select **Assign an existing license key to this vCenter Server** and select a license key from the Product list.
- Select **Assign a new license key to this vCenter Server**, click **Enter Key**, and enter a vCenter Server license key and an optional label for the key.

  NOTE To enter ESXi host license keys, select **View > Administration > Licensing**

  .

Configure Statistics Intervals

Statistic intervals determine the frequency at which statistic queries occur, the length of time statistical data is stored in the database, and the type of statistical data collected.

Required privilege: **Global.Settings**

NOTE Not all interval attributes are configurable.

Prerequisites

To configure statistics settings, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 If necessary, select **Administration > Settings** to open the **vCenter Server Settings dialog box** vCenter Server.

2 In the navigation panel, select **Statistics**.

3 In the Statistics Intervals section, select or deselect a collection interval to enable or disable it.

   Enabling a longer interval automatically enables all shorter intervals.

4 To change a collection interval attribute, select its row in the Statistics Interval section and click **Edit** to open the Edit Collection Interval dialog box.

   a In **Keep Samples for**, select an archive length.

      This option is configurable only for the Day and Year intervals.

   b In **Statistics Interval**, select an interval duration.

      This option is configurable only for the Day interval.

   c In **Statistics Level** select a new level interval level.

      Level 4 uses the highest number of statistics counters. Use it only for debugging purposes.

      The statistics level must be less than or equal to the statistics level set for the preceeding statistics interval. This is a vCenter Server dependency.

5 (Optional) In the Database Size section, estimate the effect of the statistics settings on the database.

   a Enter the number of **Physical Hosts**.

   b Enter the number of **Virtual Machines**.

      The estimated space required and number of database rows required are calculated and displayed.

   c If necessary, make changes to your statistics collection settings.

6 Click **OK**.

Configure Runtime Settings

You can change the vCenter Server ID and the vCenter Server Managed IP address. Usually, you do not need to change these settings, but you might need to make changes if you run multiple vCenter Server systems in the same environment.

Required privilege: **Global.Settings**

Prerequisites

To configure runtime settings, the vSphere Client must be connected to the vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 If the vCenter Server system is part of a connected group, select the server you want to configure from the **Current vCenter Server** drop-down menu.

3 In the navigation panel, select **Runtime Settings**.

4 In **vCenter Server Unique ID**, enter a unique ID.

   You can change this value to a number from 0 through 63 to uniquely identify each vCenter Server system running in a common environment. By default, an ID value is generated randomly.

5 In **vCenter Server Managed IP**, enter the vCenter Server system IP address.

6 In **vCenter Server Name**, enter the name of the vCenter Server system.

   If you change the DNS name of the vCenter Server, use this option to modify the vCenter Server name to match.

7 Click **OK** to save your changes and close the dialog box.

What to do next

If you made changes to the vCenter Server system Unique ID, you must restart the vCenter Server system for these changes to take effect.

Configure Active Directory Settings

You can configure some of the ways vCenter Server interacts with the Active Directory server.

Required privilege: **Global.Settings**

Prerequisites

To configure active directory settings, the vSphere Client must be connected to the vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Active Directory**.

3 In **Active Directory Timeout**, enter the timeout interval in seconds for connecting to the Active Directory server.

4 Select **Enable Query Limit** to limit the number of users and groups displayed in the Add Permissions dialog box.

5 In **Users & Groups**, enter the maximum number of users and groups to display.

   If you enter 0 (zero), all users and groups appear.

6 Select **Enable Validation** to have vCenter Server periodically check its known users and groups against the Active Directory server.

7 In **Validation Period**, enter the number of minutes between instances of synchronization.

8 Click **OK** to save your changes and close the dialog box.

Configure Mail Sender Settings

You must configure the email address of the sender account in order to enable vCenter Server operations, such as sending email notifications as alarm actions.

Required privilege: **Global.Settings**

Prerequisites

To configure SMTP notifications, the vSphere Client must be connected to the vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Mail**.

3 Enter the SMTP server information.

   The SMTP Server is the DNS name or IP address of the SMTP gateway to use for sending email messages

4 Enter the sender account information.

   The Sender Account is the email message address of the sender.

   NOTE The full email address must be entered, including the domain name (the information after the @ sign).

   For example, mail_server@datacenter.com.

5 Click **OK**.

What to do next

To test the mail settings, create an alarm that can be triggered by a user action, such as an alarm triggered by powering off a virtual machine, and verify that you receive an email when the alarm is triggered.

Configure SNMP Settings

You can configure up to four receivers to receive SNMP traps from vCenter Server. For each receiver, specify a host name, port, and community.

Prerequisites

To configure SNMP settings, the vSphere Client must be connected to a vCenter Server system.

Required privilege: **Global.Settings**

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the settings list, select **SNMP**.

3 In **Receiver URL**, enter the host name or IP address of the SNMP receiver.

4 In the field next to the Receiver URL field, enter the port number of the receiver.

   The port number must be a value between 1 and 65535.

5 In **Community String**, enter the community identifier.

6 Click **OK**.

Configure Timeout Settings

You can configure the timeout intervals for vCenter Server operations. These intervals specify the amount of time after which the vSphere Client times out.

Required privilege: **Global.Settings**

Prerequisites

To configure timeout settings, the vSphere Client must be connected to the vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Timeout Settings**.

3 In **Normal Operations**, enter the timeout interval in seconds for normal operations.

   Do not set the value to zero (0).

4 In **Long Operations**, enter the timeout interval in minutes for long operations.

   Do not set the value to zero (0).

5 Click **OK**.

6 Restart the vCenter Server system for the changes to take effect.

Configure Logging Options

You can configure the amount of detail that vCenter Server collects in log files.

Required privilege: **Global.Settings**

Prerequisites

To configure statistics settings, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Logging Options**.

3 From the vCenter Server Logging list, select logging options.

Option	Description
None (Disable logging)	Turn off logging
Error (Errors only)	Display only error log entries
Warning (Errors and warnings)	Display warning and error log entries

Option	Description
Info (Normal logging)	Displays information, error, and warning log entries
Verbose (Verbose)	Displays information, error, warning, and verbose log entries
Trivia (Extended verbose)	Displays information, error, warning, verbose, and trivia log entries

4 Click **OK**.

Changes to the logging settings take effect immediately. You do not need to restart vCenter Server system.

Configure the Maximum Number of Database Connections

You can configure the maxiumum number of database connections that can occur simultaneously.

Prerequisites

To configure database settings, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Database**.

3 In **Maximum number**, type the number.

Generally, you do not need to change this value. You might want to increase this number if your vCenter Server system frequently performs many operations and performance is critical. You might want to decrease this number, if the database is shared and connections to the database are costly. VMware recommends that you not change this value unless one of these issues pertains to your system.

4 Click **OK**.

Configure Database Retention Policy

In order to limit the growth of the vCenter Server database and conserve storage space, you can configure the database to discard information about tasks or events after a specified period of time.

Do not use these options if you want to retain a complete history of tasks and events for your vCenter Server.

Prerequisites

To configure the database retention policy, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 Select **Database Retention Policy**.

3 (Optional) Select **Tasks retained for**, and type a value in days in the text box.

Information about tasks performed on this vCenter Server system will be discarded after the specified number of days.

4 (Optional) Select **Events retained for**, and type a value in days in the text box.

Information about events for this vCenter Server system will be discarded after the specified number of days.

5 Click **OK**.

Configure Advanced Settings

You can use the Advanced Settings page to modify the vCenter Server configuration file, `vpxd.cfg`.

This page can be used to add entries to the `vpxd.cfg` file, but not to edit or delete them. VMware recommends that you change these settings only when instructed to do so by VMware technical support or when you are following specific instructions in VMware documentation.

Required privilege: **Global.Settings**

Prerequisites

To configure statistics settings, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 If necessary, select **Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

2 In the navigation pane, select **Advanced Settings**.

3 In the **Key** field, type a key.

4 In the **Value** field, type the value for the specified key.

5 Click **Add**.

6 Click **OK**.

What to do next

Many advanced options changes require that the vCenter Server system be restarted before they take effect. Consult VMware technical support to determine if your changes require a restart.

Configuring Communication Among ESXi , vCenter Server, and the vSphere Client

By default, the vSphere Client uses ports 80 and 443 to communicate with vCenter Server and ESXi hosts.

Configure your firewall to allow communication between the vSphere Client and vCenter Server by opening ports 80 and 443.

vCenter Server acts as a web service. If your environment requires the use of a web proxy, vCenter Server can be proxied like any other web service.

Reboot or Shut Down an ESXi Host

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

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Shut down all virtual machines running on the ESXi host.

3 Right-click the ESXi host and select **Reboot** or **Shut Down**.

- If you select **Reboot**, the ESXi host shuts down and reboots.
- If you select **Shut Down**, the ESXi host shuts down. You must manually power the system back on.

4 Provide a reason for the shut down.

   This information is added to the log.

Organizing Your Inventory 3

Plan how you will set up your virtual environment. A large vSphere implementation might contain several virtual data centers with a complex arrangement of hosts, clusters, resource pools, and networks. Smaller implementations might require a single virtual data center with a much less complex topology. Regardless of the scale of your virtual environment, consider how the virtual machines it will support are going to be used and administered.

Here are questions you should answer as you create and organize an inventory of virtual objects:

- Will some virtual machines require dedicated resources?
- Will some virtual machines experience periodic spikes in workload?
- Will some virtual machines need to be administered as a group?
- Do you want to use multiple vSphere Standard Switches, or you want to have a single vSphere Distributed Switch per data center?
- Do you want to use vMotion and Distributed Resource Management with certain virtual machines but not others?
- Will some virtual objects require one set of system permissions, while other objects will require a different set of permissions?

The left pane of the vSphere Client displays your vSphere inventory. You can add and arrange objects in any way with the following restrictions:

- The name of an inventory object must be unique with its parent.
- vApp names must be unique within the Virtual Machines and Templates view.
- System permissions are inherited and cascade.

Tasks for Organizing Your Inventory

Populating and organizing your inventory involves the following activities:

- Create data centers.
- Add hosts to the data centers.
- Organize inventory objects in folders.
- Setup networking by using vSphere Standard Switches or vSphere Distributed Switches. To use services such as vMotion, TCP/IP storage, Virtual SAN, and Fault Tolerance, setup VMkernel networking for these services. For more information, see *vSphere Networking*.
- Configure storage systems and create datastore inventory objects to provide logical containers for storage devices in your inventory. See *vSphere Storage*.

- Create clusters to consolidate the resources of multiple hosts and virtual machines. You can enable vSphere HA and vSphere DRS for increased availability and more flexible resource management. See *vSphere Availability* for information about configuring vSphere HA and *vSphere Resource Management* for information about configuring vSphere DRS.
- Create resource pools to provide logical abstraction and flexible management of the resources in vSphere. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. See *vSphere Resource Management* for details.

This chapter includes the following topics:

- "Create Datacenters," on page 36
- "Add Hosts," on page 37
- "Create Clusters," on page 38
- "Create Resource Pools," on page 38
- "Create Datastores," on page 39
- "Create Host-Wide Networks," on page 40
- "Create Datacenter-Wide Networks," on page 40

Create Datacenters

A virtual datacenter is a container for all the inventory objects required to complete a fully functional environment for operating virtual machines. You can create multiple datacenters to organize sets of environments. For example, you might create a datacenter for each organizational unit in your enterprise or create some datacenters for high performance environments and others for less demanding virtual machines.

Prerequisites

- Open a vSphere Client session to a vCenter Server.
- Verify that you have sufficient permissions to create a datacenter object.

Note Inventory objects can interact within a datacenter, but interaction across datacenters is limited. For example, you can hot migrate virtual machines from one host to another host in the same datacenter, but not from a host in one datacenter to a host in a different datacenter.

Procedure

1. Go to **Home > Inventory > Hosts and Clusters**.
2. Select **File > New > Datacenter**.
3. Rename the datacenter.

What to do next

Add hosts, clusters, resource pools, vApps, networking, datastores, and virtual machines to the datacenter.

Add Hosts

You can add hosts under a datacenter object, folder object, or cluster object. If a host contains virtual machines, those virtual machines are added to the inventory together with the host. Information about configuring hosts is located in the *vSphere Networking*, *vSphere Storage*, *vSphere Security*, and *vSphere Host Profiles* documentation.

Prerequisites

- Open a vSphere Client session to a vCenter Server.
- Verify that you have sufficient permissions to create a host object.
- Verify that a Datacenter, folder, or cluster exists in the inventory.
- Obtain the user name and password for an account with administrative privileges on the host.
- Verify that hosts behind a firewall are able to communicate with the vCenter Server system and all other hosts through port 902 or other custom-configured port.
- Verify that all NFS mounts on the host are active.

Procedure

1. Select **Home > Inventory > Hosts and Clusters**.
2. Select a datacenter, cluster, or folder within a datacenter.
3. Select **File > New > Add Host**.
4. Enter host name or IP address and administrator credentials and click **Next**.
5. (Optional) Select **Enable Lockdown Mode** to disable remote access for the administrator account after vCenter Server takes control of this host.

   Selecting this check box ensures that the host is managed only through vCenter Server. You can perform certain management tasks while in lockdown mode by logging into the local console on the host.
6. Review host information and click **Next**.
7. (Optional) Assign a license key to the host if needed and click **Next**.
8. Do one of the following:

Option	Description
If you are adding the host to a cluster	Select a resource pool option and click **Next**.
If you are not adding the host to a cluster	Select a location where you want to place virtual machines that already exist on the host and click **Next**.

9. Review the summary information and click **Finish**.

The host and its virtual machines are added to the inventory.

Create Clusters

A cluster is a group of hosts. When a host is added to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it. Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.

Prerequisites

- Open vSphere Client session to a vCenter Server.
- Verify that you have sufficient permissions to create a cluster object.
- Verify that a Datacenter, or folder within a datacenter, exists in the inventory.

Procedure

1 Right-click a datacenter or folder in the vSphere Client and select **New Cluster**.

2 Enter a name for the cluster.

3 Choose cluster features.

Option	Description
If you chose to use DRS with this cluster	a Click the **vSphere DRS** box. b Select an automation level and a migration level and click **Next**. c Select a default power management setting and a DPM threshold, and click **Next**.
If you chose to use HA with this cluster	a Click **vSphere HA**. b Select whether to enable host monitoring and admission control. c If admission control is enabled, specify a policy. d Click **Next**. e Specify cluster default behavior and click **Next**. f Specify virtual machine monitoring settings and click **Next**.

4 Select an Enhanced vMotion Compatibility (EVC) setting and click **Next**.

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

5 Select a swap file policy and click **Next**.

6 Review the options you selected for the cluster and click **Finish**.

The cluster is added to the inventory.

What to do next

Add hosts and resource pools to the cluster.

Create Resource Pools

You can use resource pools to hierarchically partition available CPU and memory resources of a standalone host or a cluster. Use resource pools to aggregate resources and set allocation policies for multiple virtual machines, without the need to set resources on each virtual machine.

Prerequisites

- Verify that the vSphere Client is connected to a vCenter Server system.
- Make sure you have permissions sufficient to create a resource pool object.

- Verify that a cluster, vApp, or other resource pool object is parent to the resource pool.

Procedure

1 Select **Home > Inventory > Hosts and Clusters**.

2 Select a cluster, vApp, or resource pool.

3 Select **File > New > Resource Pool**.

4 Enter a name and specify resource settings.

5 Click **OK**.

The resource pool is added to the inventory.

What to do next

Add virtual machines and vApps to your resource pool.

Create Datastores

A datastore is a logical container that holds virtual machine files and other files necessary for virtual machine operations. Datastores can exist on different types of physical storage, including local storage, iSCSI, Fibre Channel SAN, or NFS. A datastore can be VMFS-based or NFS-based.

Prerequisites

- Open a vSphere Client session to a vCenter Server.
- Verify that you have sufficient permissions to create a datastore object.
- Verify that at least one host in the inventory has access to physical storage.

Procedure

1 Select **Home > Inventory > Datastores**.

2 Right-click on a datacenter and select **Add Datastore**.

3 Select a host and click **Next**.

4 Select a type of storage and click **Next**.

Option	Description
Disk or LUN	a Select a disk or LUN and click **Next**. b Review the disk layout information and click **Next**. c Enter a name for the datastore and click **Next**. d Specify maximum file and block sizes. e Specify disk or LUN capacity and click **Next**.
Network File System	a Enter server and folder information. b Select whether clients should mount the NFS as read-only. c Enter a name and click **Next**.

5 Review summary information and click **Finish**.

A datastore is added to the inventory.

Create Host-Wide Networks

In vSphere, you can create standard networks and distributed networks. Standard networks provide a method of communication among the virtual machines on a standalone host and consist of standard switches and port groups. Distributed networks aggregate the networking capabilities of multiple hosts and enable virtual machines to keep consistent network configuration as they migrate across hosts. Distributed networks consist of vSphere Distributed Switches, uplink port groups, and port groups.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to create a standard switch.
- Verify that a host exists in the inventory.

Procedure

1. Select a host from the inventory.
2. Click the **Configuration** tab.
3. In the Hardware section, click **Networking**.
4. Click **vSphere Standard Switch**.
5. Click **Add Networking**.
6. Select a connection type and click **Next**.
7. Select an existing virtual switch or create one and click **Next**.
8. Enter a display label for the port group on the switch.
9. Select a VLAN ID and click **Next**.
10. Review your settings and click **Finish**.

If you chose to use an existing standard switch, a new port group is added to it. If you chose to create a standard switch, it is added with a port group.

Create Datacenter-Wide Networks

In vSphere, you can create standard networks and distributed networks. Standard networks provide a method of communication among the virtual machines on a standalone host and consist of standard switches and port groups. Distributed networks aggregate the networking capabilities of multiple hosts and enable virtual machines to keep consistent network configuration as they migrate across hosts. Distributed networks consist of vSphere Distributed Switches, uplink port groups, and port groups.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to create a distributed switch.
- Verify that a host exists in the inventory.

Procedure

1. Select **Home > Inventory > Networking** view, and select a data center.
2. Right-click on the data center and select **New vSphere Distributed Switch**.
3. Select the vSphere Distributed Switch Version and click **Next**.

4 In the General section, type a name for the switch.

5 Specify the maximum number of uplink ports (physical adapters per host) and click **Next**.

6 Select **Add now** to add hosts and their physical adapters to the switch.

   Select **Add later** to add hosts and their physical adapters to the switch after the vSphere Distributed Switch has been created.

7 Select the hosts to add in the **Host/Physical adapters** section and click **Next**.

8 Select **Automatically create a default port group** to automatically create a port group and click **Finish**.

A vSphere Distributed Switch, with its associated uplink ports and port groups, is added to the inventory.

What to do next

- Add hosts to the switch.
- Add port groups to the switch.
- Edit switch properties.

Edit General vSphere Distributed Switch Settings

You can edit the general settings for a vSphere distributed switch, such as the distributed switch name and the number of uplink ports on the distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select **General** to edit the vSphere distributed switch settings.

Option	Description
Name	Type the name for the distributed switch.
Number of Uplink Ports	Select the number of uplink ports for the distributed switch.
Notes	Type any notes for the distributed switch.

4 (Optional) Edit uplink port names.

   a Click **Edit uplink names**.

   b Type new names for one or more uplink ports.

   c Click **OK**.

5 Click **OK**.

Edit Advanced vSphere Distributed Switch Settings

You can change advanced vSphere distributed switch settings such as Cisco Discovery Protocol and the maximum MTU for the vSphere distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.

- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select **Advanced** to edit the following vSphere distributed switch settings.

Option	Description
Maximum MTU	Maximum MTU size for the vSphere distributed switch.
Discovery Protocol Status	Choose the status for discovery protocol on the vSphere distributed switch. ■ **Enabled**. Enabled discovery protocol for the vSphere distributed switch. 1 Select **Cisco Discovery Protocol** or **Link Layer Discovery Protocol** from the **Type** drop-down menu. 2 Set **Operation** to **Listen**, **Advertise**, or **Both**. ■ **Disabled**.
Admin Contact Info	Enter the **Name** and **Other Details** for the vSphere distributed switch administrator.

4 Click **OK**.

Add Hosts to a vSphere Distributed Switch

You can add hosts and physical adapters to a vSphere distributed switch at the distributed switch level after it is created.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Add Host**.

3 Select the hosts to add.

4 Under the selected hosts, select the physical adapters to add and click **Next**.

You can select physical adapters that are not being used and physical adapters that are being used.

Note Moving a physical adapter to a distributed switch without moving any associated virtual adapters can cause those virtual adapters to lose network connectivity.

5 For each virtual adapter, select **Destination port group** and select a port group from the drop-down menu to migrate the virtual adapter to the distributed switch or select **Do not migrate**.

6 (Optional) Set the maximum number of ports on a host.

a Click **View Details** for the host.

b Select the maximum number of ports for the host from the drop-down menu.

c Click **OK**.

7 Click **Next**.

8 (Optional) Migrate virtual machine networking to the distributed switch.

   a Select **Migrate virtual machine networking**.

   b For each virtual machine, select **Destination port group** and select a port group from the drop-down menu or select **Do not migrate**.

9 Click **Next**.

10 (Optional) If you need to make any changes, click **Back** to the appropriate screen.

11 Review the settings for the distributed switch and click **Finish**.

Add a Distributed Port Group

Add a distributed port group to a vSphere distributed switch to create a distributed switch network for your virtual machines.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane and select **New Port Group**.

3 Enter a **Name** and the **Number of Ports** for your new distributed port group.

4 Select a VLAN Type.

Option	Description
None	Do not use VLAN.
VLAN	In the **VLAN ID** field, enter a number between 1 and 4094.
VLAN Trunking	Enter a VLAN trunk range.
Private VLAN	Select a private VLAN entry. If you did not create any private VLANs, this menu is empty.

5 Click **Next**.

6 Click **Finish**.

Edit General Distributed Port Group Settings

You can edit general distributed port group settings such as the distributed port group name and port group type.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **General** to edit the following distributed port group settings.

Option	Action
Name	Type the name for the distributed port group.
Description	Type a brief description of the distributed port group.
Number of Ports	Type the number of ports on the distributed port group.
Port binding	Choose when ports are assigned to virtual machines connected to this distributed port group. ■ Select **Static binding** to assign a port to a virtual machine when the virtual machine connects to the distributed port group. This option is not available when the vSphere Client is connected directly to ESXi. ■ Select **Dynamic binding** to assign a port to a virtual machine the first time the virtual machine powers on after it is connected to the distributed port group. Dynamic binding is deprecated in ESXi 5.x. ■ Select **Ephemeral** for no port binding. This option is not available when the vSphere Client is connected directly to ESXi.

4 Click **OK**.

Edit Advanced Distributed Port Group Settings

You can edit advanced distributed port group settings, such as override settings and reset at disconnect.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Advanced** to edit the distributed port group properties.

Option	Description
Allow override of port policies	Select this option to allow distributed port group policies to be overridden on a per-port level. Click **Edit Override Settings** to select which policies can be overridden at the port level.
Edit Override Settings	Select which policies can be overridden at the port level.
Configure reset at disconnect	When a distributed port is disconnected from a virtual machine, the configuration of the distributed port is reset to the distributed port group setting. Any per-port overrides are discarded.

4 Click **OK**.

Managing License Keys in the vSphere Client

4

Use the vSphere Client to manage license keys directly on individual ESXi hosts or centrally in the license inventory of a vCenter Server system.

This chapter includes the following topics:

- "Licensing Limitations in the vSphere Client," on page 45
- "Managing License Keys on ESXi Hosts," on page 45
- "Managing License Keys on vCenter Server," on page 47

Licensing Limitations in the vSphere Client

The licensing tasks that you can perform when you connect directly to an ESXi host or vCenter Server system with the vSphere Client are limited

The following licensing features are unavailable in the vSphere Client:

- License Reporting

Use the vSphere Web Client as the primary interface for managing the full range of licensing functions available in your vSphere 6.0 environment.

Managing License Keys on ESXi Hosts

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

Access the ESXi License Key and Licensed Features in the vSphere Client

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

Procedure

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

   The license key and a list of features that you can configure on the host appears. The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Assign a License Key to an ESXi Host

Using the vSphere Client, you can assign an existing or new license key to an ESXi host.

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

Prerequisites

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

Procedure

1 In the vSphere Client, select the host in the inventory and click the **Configuration** tab.

2 In the Software section, click **Licensed Features** and click **Edit**.

3 Assign a license key.

- Select **Assign an existing license key to this host** and select a license key from the **Product** list.
- Select **Assign a new license key to this host**, click **Enter Key**, and specify a license key in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

4 Click **OK**.

Set an ESXi Host to Evaluation Mode

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

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 In the Software section, click **Licensed Features**.

4 Click **Edit** next to ESX Server License Type.

5 Click **Product Evaluation**.

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

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

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

The License Key of an ESXi Host is Replaced

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

Problem

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

Cause

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

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

Solution

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

Managing License Keys on vCenter Server

vSphere license management is centralized. You can use the vSphere Client to manage all licenses that are available in the license inventory of a vCenter Server system.

Access vCenter Server License Keys and Features

You can access the license keys and features available in the vCenter Server license inventory from the Licensing page in the vSphere Client.

Prerequisites

- Verify that you have the **Global.Licenses** privilege.
- Ensure that the vSphere Client is connected to the vCenter Server system.

Procedure

1. In the vSphere Client, select **View > Administration > Licensing**.

   You can view and manage the license keys available in the vCenter Server inventory from the **Management** tab.

2. (Optional) Click **Refresh**.
3. In the **Management** tab, select a sorting option for the license information.

Option	Description
Product	Displays the available license keys listed by product.
License key	Displays the available license keys listed by license key.
Asset	Displays the available license keys listed by the asset to which they are assigned: host, vCenter Server, or solution.

The **Management** tab displays the available license keys listed by product, license key, or asset. You can right-click any of the listed items to add, assign, and remove license keys and copy license information to your clipboard.

What to do next

If you have a license key with zero assigned capacity, you can:

- Assign the license key to assets that require licensing.
- Remove the license key if the key is no longer required.

You should not keep unassigned license keys in the vCenter Server license inventory.

Add License Keys to the vCenter Server License Inventory

After you obtain license keys, you can add them to the vCenter Server license inventory. You can add multiple license keys at the same time.

Prerequisites

- Verify that you have the **Global.Licenses** privilege.
- Ensure that the vSphere Client is connected to the vCenter Server system.

Procedure

1. In the vSphere Client, select **Home > Administration > Licensing**.
2. Click **Manage vSphere Licenses**.
3. In the **Add License Keys** text area, specify license keys one per line.

   You can specify a list of keys in one operation.
4. (Optional) Type a brief label of the keys.
5. Click **Add License Keys**.

   If you specify any invalid license keys, you receive an error message that lists only the invalid keys. You can either delete the invalid keys, or add them after correcting them.
6. If you are not ready to assign the license keys to assets, click **Next** through the remaining wizard screens and click **Finish** to save your changes.

The license keys are added to the vCenter Server license inventory.

What to do next

Assign the license keys to assets that require licensing. You should not keep unassigned license keys in the vCenter Server license inventory.

Assign a License Key to Assets

You can assign license keys to single or multiple assets, individually, or in batches.

Note If an ESXi host disconnects from vCenter Server immediately after you assign a license key, the license assignment operation does not complete but the host appears as licensed. The host is licensed after it reconnects to vCenter Server.

Prerequisites

- Verify that you have the **Global.Licenses** privilege.
- Ensure that the vSphere Client is connected to the vCenter Server system.

Procedure

1 In the vSphere Client, select **Home > Administration > Licensing**.

2 Click **Manage vSphere Licenses**.

3 Click **Next** to go to the Assign Licenses page.

4 Click the **ESX**, **vCenter Server**, or **Solutions** tab to display the available assets.

5 Select the assets to show.

6 In the Asset window, select one or more assets to license.

   To select multiple assets, use Ctrl-click or Shift-click.

7 In the Product window, select an appropriate license key and click **Next**.

   If the license key you assign has a strong limit, the license capacity must be greater than or equal to the required license use for the asset. Otherwise, you cannot assign the license key. Check the EULA of the license to determine whether it has a strong limit.

8 (Optional) If you are not ready to remove any license keys, click **Next** to skip the Remove License Keys page and click **Finish** to save your changes.

Add a License Key and Assign It to an Asset

After you obtain a license key, you can add it to the vCenter Server license inventory and assign the license key to assets.

Prerequisites

- Verify that you have the **Global.Licenses** privilege.
- Ensure that the vSphere Client is connected to the vCenter Server system.

Procedure

1 In the vSphere Client, select **Home > Administration > Licensing**.

2 In the **Management** tab, select **Asset** as a primary entity for sorting the license information.

3 Right-click an asset and select **Change license key**.

4 Select **Assign a new license key** and click **Enter Key**.

5 Specify the license key, type an optional label for the key, and click **OK**.

6 Click **OK**.

The license key is added to the vCenter Server license inventory and assigned to the corresponding asset.

What to do next

Assign the license key to other assets of the same type in case the license key has available capacity.

Export License Information

You can export license information in a file that you can later open with third-party applications.

Prerequisites

- Verify that you have the **Global.Licenses** privilege.
- Ensure that the vSphere Client is connected to the vCenter Server system.

Procedure

1 In the vSphere Client, select **Home > Administration > Licensing**.

2 In the **Management** tab, select the view that you want to export.

- **Product**
- **License key**
- **Asset**

3 Click **Export**.

4 In the Save As dialog box, select a folder, a filename, and a format for the exported license data and click **Save**.

Managing Tasks 5

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

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

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

This chapter includes the following topics:

- "Viewing Tasks," on page 51
- "Cancel a Task," on page 53
- "Schedule Tasks," on page 53
- "Policy Rules for Task Operations," on page 57

Viewing Tasks

You can view tasks that are associated with a single object or all objects in the vSphere Client inventory. The **Tasks & Events** tab lists completed tasks and tasks that are currently running.

By default, the tasks list for an object also includes tasks performed on its child objects. You can filter the list by removing tasks performed on child objects and by using keywords to search for tasks.

View All Tasks

You view completed tasks and running tasks in the vSphere Client **Tasks & Events** tab.

Prerequisites

- Open a vSphere Client session to a vCenter Server.

Procedure

1 In the vSphere Client, select the object in the inventory.

2 Display the tasks for a single object or the entire vCenter Server.
   - To display the tasks for a single object, select the object.
   - To display the tasks in the vCenter Server, select the root folder.
3 Click the **Tasks & Events** tab.

   The task list contains tasks performed on the object and its children.
4 (Optional) To view detailed information for a task, select the task in the list.

   The **Task Details** pane displays details such as task status, any error messages in the error stack, and any related events.

View Recent Tasks

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

Procedure

1 In the vSphere Client, select the host from the inventory.
2 If necessary, select **View > Status Bar** to display the status bar at the bottom of the vSphere Client.

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

View Scheduled Tasks

You view scheduled tasks in the vSphere Client **Scheduled Tasks** pane. The scheduled task list includes tasks that are scheduled to run and those that have already run.

Prerequisites

- Open a vSphere Client session to a vCenter Server.

Procedure

◆ In the vSphere Client, select **Home > Management > Scheduled Tasks**.

Filter Tasks for a Host or Datacenter

Filtering the task list removes tasks performed on child objects.

Prerequisites

- Open a vSphere Client session to a vCenter Server.

Procedure

1 In the vSphere Client, select the host or datacenter in the inventory and click the **Tasks & Events** tab.
2 In **View**, click **Tasks** to display the tasks list.
3 If the **Show all entries** list and the search field are not displayed under the **Tasks** and **Events** buttons, select **View > Filtering**.
4 Click **Show all entries** and select **Show host entries** or **Show datacenter entries**, depending on the object selected.

Use Keywords to Filter the Tasks List

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

Prerequisites

- Open a vSphere Client session to a vCenter Server.

Procedure

1. In the vSphere Client, select the object in the inventory.
2. If the **Name, Target or Status contains** search field is not displayed above the Recent Tasks pane, select **View > Filtering**.
3. Click the search field arrow and select the attributes to include in the search.
4. Type a keyword into the box and press Enter.

Cancel a Task

Canceling a task stops a running task from occurring. Canceling a scheduled task does not cancel subsequent runs. To cancel a scheduled task that has not run, reschedule it.

Note You can only cancel a subset of tasks by using the vSphere Client.

Required privileges:

- Manual tasks: **Tasks.Update Task**
- Scheduled tasks:**Scheduled Task.Remove Task**
- Appropriate permissions on the host where the task is running

Prerequisites

- Open a vSphere Client session to a vCenter Server.

Procedure

1. Locate the task in the **Recent Tasks** pane of the **Status Bar**.

   By default, the **Status Bar** is displayed at the bottom of the vSphere Client. If it is not visible, select **View > Status Bar**.

2. Right-click the appropriate task and select **Cancel**.

   If the cancel option is unavailable, the selected task cannot be canceled.

The vCenter Server system or ESXi host stops the progress of the task and returns the object to its previous state. The vSphere Client displays the task with a **Canceled** status.

Schedule Tasks

You can schedule tasks to run once in the future or multiple times, at a recurring interval.

The tasks you can schedule are listed in the following table.

Table 5-1. Scheduled Tasks

Scheduled Task	Description
Add a host	Adds the host to the specified data center or cluster.
Change the power state of a virtual machine	Powers on, powers off, suspends, or resets the state of the virtual machine.
Change cluster power settings	Enable or disable DPM for hosts in a cluster.
Change resource settings of a resource pool or virtual machine	Changes the following resource settings: ■ CPU – Shares, Reservation, Limit. ■ Memory – Shares, Reservation, Limit.
Check compliance of a profile	Checks that a host's configuration matches the configuration specified in a host profile.
Clone a virtual machine	Makes a clone of the virtual machine and places it on the specified host or cluster.
Create a virtual machine	Creates a new virtual machine on the specified host.
Deploy a virtual machine	Creates a new virtual machine from a template on the specified host or cluster.
Migrate a virtual machine	Migrate a virtual machine to the specified host or datastore by using migration or migration with vMotion.
Make a snapshot of a virtual machine	Captures the entire state of the virtual machine at the time the snapshot is taken.
Scan for Updates	Scans templates, virtual machines, and hosts for available updates. This task is available only when vSphere Update Manager is installed.
Remediate	Installs missing patches from the baselines selected for remediation on the hosts discovered during the scan operation and applies the newly configured settings. This task is available only when vSphere Update Manager is installed.

You create scheduled tasks by using the Scheduled Task wizard. For some scheduled tasks, this wizard opens the wizard used specifically for that task. For example, if you create a scheduled task that migrates a virtual machine, the Scheduled Task wizard opens the Migrate Virtual Machine wizard, which you use to set up the migration details.

Scheduling one task to run on multiple objects is not possible. For example, you cannot create one scheduled task on a host that powers on all virtual machines on that host. You must create a separate scheduled task for each virtual machine.

After a scheduled task runs, you can reschedule it to run again at another time.

Create a Scheduled Task

To schedule a task, use the Scheduled Task wizard.

Required privilege: **Schedule Task.Create Tasks**

You can schedule a limited number of tasks by using the vSphere Client. If the task to schedule is not available, use the vSphere API. See the vSphere SDK *Programming Guide*.

Caution Do not schedule multiple tasks to be performed at the same time on the same object. The results are unpredictable.

Prerequisites

The vSphere Client must be connected to a vCenter Server system to schedule tasks.

Procedure

1 In the navigation bar, click **Home > Management > Scheduled Tasks**.

The current list of scheduled tasks appears.

2 In the toolbar, click **New**.

3 In the Select a Task to Schedule dialog box, select a task and click **OK** to open the wizard for that task.

NOTE For some scheduled tasks, the wizard opens the wizard used specifically for that task. For example, to migrate a virtual machine, the Scheduled Task wizard opens the Migrate Virtual Machine Wizard, which you use to set up the migration details.

4 Complete the wizard that opens for the task.

5 In the Schedule Task section, enter a task name and task description.

6 Select a **Frequency** and specify a **Start Time**.

You can schedule a task to run only once during a day. To set up a task to run multiple times in one day, set up additional scheduled tasks.

Table 5-2. Scheduled Task Frequency Options

Frequency	Action
Once	■ To run the scheduled task immediately, select **Now** and click **Next**. ■ To run the scheduled task at a later time and date, select **Later** and enter a **Time**. Click the **Date** arrow to display the calendar and click a date.
After Startup	■ In **Delay**, enter the number of minutes to delay the task.
Hourly	1 In **Start Time**, enter the number of minutes after the hour to run the task. 2 In **Interval**, enter the number of hours after which to run the task. For example, to start a task at the half-hour mark of every 5th hour, enter **30** and **5**.
Daily	■ Enter the **Start Time** and **Interval**. For example, to run the task at 2:30 pm every four days, enter **2:30** and **4**.
Weekly	1 Enter the **Interval** and **Start Time**. 2 Select each day on which to run the task. For example, to run the task at 6 am every Tuesday and Thursday, enter **1** and **6 am**, and select **Tuesday** and **Thursday**.
Monthly	1 Enter the **Start Time**. 2 Specify the days by using one of the following methods. ■ Enter a specific date of the month. ■ Select **first**, **second**, **third**, **fourth**, or **last,** and select the day of the week. **last** runs the task on the last week in the month that the day occurs. For example, if you select the last Monday of the month and the month ends on a Sunday, the task runs six days before the end of the month. 3 In **Interval**, enter the number of months between each task run.

7 Click **Next**.

8 Set up email notifications and click **Next**.

9 Click **Finish**.

The vCenter Server system adds the task to the list in the **Scheduled Tasks** window.

Change or Reschedule a Task

After a scheduled task is created, you can change the timing, frequency, and specifics of the task. You can edit and reschedule tasks before or after they run.

Required privilege:**Schedule Task.Modify Task**

Prerequisites

- Open a vSphere Client session to a vCenter Server system.

Procedure

1. In the vSphere Client, click **Home > Management > Scheduled Tasks**.
2. Select the task.
3. In the toolbar, click **Properties**.
4. Change task attributes as necessary.
5. Click **Next** to advance through the wizard.
6. Click **Finish**.

Remove a Scheduled Task

Removing a scheduled task removes all future occurrences of the task. The history associated with all completed occurrences of the task remains in the vCenter Server database.

Prerequisites

To remove scheduled tasks, the vSphere Client must be connected to the vCenter Server system.

Required privilege:**Scheduled Task.Remove Task**

Procedure

1. In the vSphere Client, click **Home > Management > Scheduled Tasks**.
2. Select the task.
3. Select **Inventory > Scheduled Task > Remove**.
4. Click **OK**.

The task is removed from the list of scheduled tasks.

Canceling Scheduled Tasks

Canceling a task stops a running task from occurring, regardless of whether the task was a real-time task or a scheduled task. The operation cancels only the running task. If the task being canceled is a scheduled task, subsequent runs are not canceled.

Tasks that aren't running can be cleared when they are in a queued or scheduled state. In such cases, because the cancel operation is not available, either remove the task or reschedule it to run at a different time. Removing a scheduled task requires that you recreate it to run it in the future, rescheduling does not.

You can cancel the following tasks:

- Connecting to a host
- Cloning a virtual machine
- Deploying a virtual machine

- Migrating a powered off virtual machine. This task is cancelable only when the source disks have not been deleted.

If your vSphere environment uses virtual services, you can also cancel the following scheduled tasks:

- Change the power state of a virtual machine
- Make a snapshot of a virtual machine

Policy Rules for Task Operations

The vCenter Server system and ESXi hosts adhere to certain rules when managing tasks.

The vCenter Server system and ESXi hosts use the following rules to process tasks:

- The user performing the task in the vSphere Client must have the correct permissions on the relevant objects. After a scheduled task is created, it will be performed even if the user no longer has permission to perform the task.
- When the operations required by manual tasks and scheduled tasks conflict, the activity due first is started first.
- When a virtual machine or host is in an incorrect state to perform any activity, manual or scheduled, vCenter Server or the ESXi host does not perform the task. A message is recorded in the log.
- When an object is removed from the vCenter Server or the ESXi host, all associated tasks are also removed.
- The vSphere Client and vCenter Server system use UTC time to determine the start time of a scheduled task. This ensures vSphere Client users in different time zones see the task scheduled to run at their local time.

Events are logged in the event log at start and completion of a task. Any errors that occur during a task are also recorded in the event log.

Caution Do not schedule multiple tasks to be performed at the same time on the same object. The results are unpredictable.

Securing the Management Interface 6

Secure the management Interface of an ESXi host and the virtual machine guest operating system by restricting the services and management agents that are allowed to interface directly with the host or virtual machine.

This chapter includes the following topics:

- "Securing ESXi Hosts," on page 59
- "Securing Virtual Machines," on page 63

Securing ESXi Hosts

The ESXi hypervisor architecture has many built-in security features such as CPU isolation, memory isolation, and device isolation. You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.

An ESXi host is also protected with a firewall. You can open ports for incoming and outgoing traffic as needed, but should restrict access to services and ports. Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment. Starting with vSphere 6.0, ESXi hosts participate in the certificate infrastructure. Hosts are provisioned with certificate that are signed by the VMware Certificate Authority (VMCA) by default.

See the VMware white paper *Security of the VMware vSphere Hypervisor* for additional information on ESXi security.

Allow or Deny Access to an ESXi Service or Management Agent

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

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

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

Procedure

1 Select the host in the inventory panel.

2 Click the **Configuration** tab, then in the Software section, click **Security Profile**.

The vSphere Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.

3 In the Firewall section, click **Properties**.

   The Firewall Properties dialog box lists all the rule sets that you can configure for the host.

4 Select the rule sets to enable, or deselect the rule sets to disable.

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

5 Click **OK**.

Add Allowed IP Addresses

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

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

Procedure

1 Select the host in the inventory panel.

2 Click the **Configuration** tab and click **Security Profile**.

3 In the Firewall section, click **Properties**.

4 Select a service in the list and click **Firewall**.

5 Select **Only allow connections from the following networks** and enter the IP addresses of networks that are allowed to connect to the host.

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

6 Click **OK**.

Set Service or Client Startup Options

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

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab, then under **Software** click **Security Profile**.

3 In the Firewall section, click **Properties**.

   All the firewall services and management agents that you can configure for the host are listed.

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

   You can set the service start policy, verify the status of the service, and manually start, stop, or restart the service through this configuration.

5 Select a policy from the **Startup Policy** list.

6 Click **OK**.

Using the ESXi Shell

The ESXi Shell (formerly Tech Support Mode or TSM) is disabled by default on ESXi hosts. You can enable local and remote access to the shell if necessary.

Enable the ESXi Shell for troubleshooting only. The ESXi Shell can be enabled and disabled whether or not the host is running in lockdown mode. See the *vSphere Security* publication for more information on lockdown mode behavior.

ESXi Shell	Enable this service to access the ESXi Shell locally.
SSH	Enable this service to access the ESXi Shell remotely using SSH. You can upload SSH keys to your hosts. See the *vSphere Security* publication for more information on SSH keys.
Direct Console UI (DCUI)	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 vSphere Client or by enabling the ESXi Shell.

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

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

Use the vSphere Client to Enable Access to the ESXi Shell

Use the vSphere Client to enable local and remote access to the ESXi Shell.

Procedure

1. Select the host in the inventory panel.
2. Click the **Configuration** tab and click **Security Profile**.
3. In the Services section, click **Properties**.
4. Select a service from the list.
   - ESXi Shell
   - SSH
   - Direct Console UI
5. Click **Options** and select **Start and stop manually**.

   When you select **Start and stop manually**, the service does not start when you reboot the host. If you want the service to start when you reboot the host, select **Start and stop with host**.
6. Select **Start** to enable the service.
7. Click **OK**.

Create a Timeout for ESXi Shell Availability

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

The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

Procedure

1 Select the host in the inventory and click the **Configuration** tab.

2 Under Software, select **Advanced Settings**.

3 In the left panel, select **UserVars**.

4 In the UserVars.ESXiShellTimeOut field, enter the availability timeout setting.

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

5 Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminated, users are not allowed to log in.

Create a Timeout for Idle ESXi Shell Sessions

If a user enables the ESXi Shell on a host, but forgets to log out of the session, the idle session remains connected indefinitely. The open connection can increase the potential for someone to gain privileged access to the host. You can prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the ESXi Shell and do not affect existing sessions.

Procedure

1 Select the host in the inventory and click the **Configuration** tab.

2 Under Software, select **Advanced Settings**.

3 In the left panel, select **UserVars**.

4 In the UserVars.ESXiShellInteractiveTimeOut field, enter the availability timeout setting.

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

5 Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminated, users are not allowed to log in.

Enable Lockdown Mode in the vSphere Client

Enable lockdown mode to require that all configuration changes go through vCenter Server. You can also enable or disable lockdown mode through the direct console user interface.

Prerequisites

- Open a vSphere Client session to a vCenter Server system.

Procedure

1 Select the host in the inventory panel.

2 Click the **Configuration** tab and click **Security Profile**.

3 Click the **Edit** link next to lockdown mode.

   The Lockdown Mode dialog box appears.

4 Select **Enable Lockdown Mode**.

5 Click **OK**.

Securing Virtual Machines

The guest operating system that runs in the virtual machine is subject to the same security risks as a physical system. Secure virtual machines as you would secure physical machines.

1 Prevent Virtual Disk Shrinking on page 63

   Nonadministrative users in the guest operating system are able to shrink virtual disks. Shrinking a virtual disk reclaims the disk's unused space. However, if you shrink a disk repeatedly, the disk can become unavailable or cause a Denial of Service (DoS). To prevent this, disable the ability to shrink virtual disks.

2 Disable Copy and Paste Operations Between Guest Operating System and Remote Console on page 64

   Copy and paste operations between the guest operating system and remote console are disabled by default. For a secure environment, retain the default setting. If you require copy and paste operations, you must enable them using the vSphere Client.

3 Modify Guest Operating System Variable Memory Limit on page 64

   You can increase the guest operating system variable memory limit if large amounts of custom information are being stored in the configuration file.

4 Prevent the Guest Operating System Processes from Sending Configuration Messages to the Host on page 65

   You can prevent guests from writing any name-value pairs to the configuration file that are sent to the host. This is appropriate when guest operating systems must be prevented from modifying configuration settings.

5 Prevent a Virtual Machine User or Process from Disconnecting Devices on page 65

   Users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. To increase virtual machine security, remove these devices. If you do not want to permanently remove a device, you can prevent a virtual machine user or process from connecting or disconnecting the device from within the guest operating system.

6 Configure Syslog on ESXi Hosts on page 66

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

Prevent Virtual Disk Shrinking

Nonadministrative users in the guest operating system are able to shrink virtual disks. Shrinking a virtual disk reclaims the disk's unused space. However, if you shrink a disk repeatedly, the disk can become unavailable or cause a Denial of Service (DoS). To prevent this, disable the ability to shrink virtual disks.

Prerequisites

Turn off the virtual machine.

Procedure

1 Log in to the vCenter Server system using the vSphere Client.

2 Select the virtual machine in the inventory.

3 On the **Summary** tab, click **Edit Settings**.

4 Select **Options > Advanced > General** and click **Configuration Parameters**.

5 Add or edit the following parameters.

Name	Value
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

6 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

When you disable this feature, you cannot shrink virtual machine disks when a datastore runs out of space.

Disable Copy and Paste Operations Between Guest Operating System and Remote Console

Copy and paste operations between the guest operating system and remote console are disabled by default. For a secure environment, retain the default setting. If you require copy and paste operations, you must enable them using the vSphere Client.

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client, select the virtual machine.

2 On the **Summary** tab, click **Edit Settings**.

3 Select **Options > Advanced > General** and click **Configuration Parameters**.

4 Ensure that the following values are in the Name and Value columns, or click **Add Row** to add them.

Name	Value
isolation.tools.copy.disable	TRUE
isolation.tools.paste.disable	TRUE

These options override any settings made in the guest operating system's VMware Tools control panel.

5 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

6 (Optional) If you made changes to the configuration parameters, restart the virtual machine.

Modify Guest Operating System Variable Memory Limit

You can increase the guest operating system variable memory limit if large amounts of custom information are being stored in the configuration file.

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client, select the virtual machine in the inventory panel.

2 On the **Summary** tab, click **Edit Settings**.

3 Select **Options > Advanced > General** and click **Configuration Parameters**.

4 If the size limit attribute is not present, you must add it.

   a Click **Add Row**.

   b In the Name column, type `tools.setInfo.sizeLimit`.

   c In the Value column, type `Number of Bytes`.

   If the size limit attribute exists, modify it to reflect the appropriate limits.

5 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

Prevent the Guest Operating System Processes from Sending Configuration Messages to the Host

You can prevent guests from writing any name-value pairs to the configuration file that are sent to the host. This is appropriate when guest operating systems must be prevented from modifying configuration settings.

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client, select the virtual machine in the inventory panel.

2 On the **Summary** tab, click **Edit Settings**.

3 Click **Options > Advanced > General**, and click **Configuration Parameters**.

4 Click **Add Row** and type the following values in the Name and Value columns.

   - In the Name column: `isolation.tools.setinfo.disable`
   - In the Value column: `true`

5 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

Prevent a Virtual Machine User or Process from Disconnecting Devices

Users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. To increase virtual machine security, remove these devices. If you do not want to permanently remove a device, you can prevent a virtual machine user or process from connecting or disconnecting the device from within the guest operating system.

Prerequisites

Turn off the virtual machine.

Procedure

1 Log in to a vCenter Server system using the vSphere Client and select the virtual machine.

2 On the **Summary** tab, click **Edit Settings**.

3 Select **Options > Advanced > General** and click **Configuration Parameters**.

4 Add or edit the following parameters.

Name	Value
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

These options override any settings made in the guest operating system's VMware Tools control panel.

5 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

6 (Optional) If you made changes to the configuration parameters, restart the virtual machine.

Configure Syslog on ESXi Hosts

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

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

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

Procedure

1 In the vSphere Client inventory, select the host.

2 Click the **Configuration** tab.

3 In the Software panel, click **Advanced Settings**.

4 Select **Syslog** in the tree control.

5 To set up logging globally, click **global** and make changes to the fields on the right.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified 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.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

6 (Optional) To overwrite the default log size and log rotation for any of the logs.

   a Click **loggers**.

   b Click the name of the log you that want to customize and enter the number of rotations and log size you want.

7 Click **OK**.

Changes to the syslog options take effect immediately.

ESXi Authentication and User Management

7

ESXi handles user authentication and supports user permissions.

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

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

This chapter includes the following topics:

- "Managing Users with the vSphere Client," on page 69
- "Assigning Permissions for ESXi," on page 72
- "Managing ESXi Roles," on page 73
- "Using Active Directory to Manage ESXi Users," on page 76
- "Use vSphere Authentication Proxy to Add a Host to a Domain," on page 77
- "Adjust the Search List in Large Domains," on page 78

Managing Users with the vSphere Client

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

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

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

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

Add an ESXi User

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

Prerequisites

- Open a vSphere Client session to an ESXi host.
- Review the password requirements as described in the *vSphere Security* publication.

Procedure

1. Log in to ESXi using the vSphere Client.

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

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

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

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

5. Click **OK**.

Modify the Settings for a User on the Host

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

Prerequisites

- Open a vSphere Client session to an ESXi host.

Procedure

1. Log in to ESXi using the vSphere Client.

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

2. Click **Users**.
3. Right-click the user and click **Edit** to open the Edit User dialog box.

4 Enter a login, a user name, and a password.

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

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

5 Click **OK**.

Remove a Local ESXi User from a Host

You can remove a local ESXi user from the host.

CAUTION Do not remove the root user.

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

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

Procedure

1 Log in to ESXi using the vSphere Client.

2 Click the **Local Users & Groups** tab and click **Users**.

3 Right-click the user to remove and select **Remove**.

Do not remove the root user for any reason.

Sort, Export, and View Local ESXi Users

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

Procedure

1 Log in to ESXi using the vSphere Client.

2 Click the **Local Users & Groups** tab and click **Users** .

3 Determine how to sort the table, and hide or show columns according to the information you want to see in the exported file.

- To sort the table by any of the columns, click the column heading.
- To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.
- To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.

4 Right-click anywhere in the table and click **Export List** to open the Save As dialog box.

5 Select a path and enter a filename.

6 Select the file type and click **OK**.

Assigning Permissions for ESXi

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

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

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

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

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

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

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

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

Permission Validation

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

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

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

Change Permissions

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

Procedure

1 From the vSphere Client, select an object in the inventory.

2 Click the **Permissions** tab.

3 Right-click the line item to select the user and role pair.

4 Select **Properties**.

5 Select a role for the user or group from the drop-down menu.

6 To propagate the privileges to the children of the assigned inventory object, click the **Propagate** check box and click **OK**.

Remove Permissions

Removing a permission for a user does not remove the user from the list of those 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.

Prerequisites

- Open a vSphere Client session to an ESXi host.

Procedure

1 From the vSphere Client, click the **Inventory** button.

2 Expand the inventory as needed and click the appropriate object.

3 Click the **Permissions** tab.

4 Click the appropriate line item to select the user and role pair.

5 Select **Inventory > Permissions > Delete**.

Change Permission Validation Settings

vCenter Server periodically validates its user and group lists against the users and groups in the Windows Active Directory domain. It then removes users or groups that no longer exist in the domain. You can change the interval between validations.

Procedure

1 From the vSphere Client connected to a vCenter Server system, select **Administration > vCenter Server Settings**.

2 In the navigation pane, select **Active Directory**.

3 (Optional) Deselect the **Enable Validation** check box to disable validation.

   Validation is enabled by default. Users and groups are validated when vCenter Server system starts, even if validation is disabled.

4 If validation is enabled, enter a value in the Validation Period text box to specify a time, in minutes, between validations.

Managing ESXi Roles

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

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

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

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

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

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

Create a Role

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

Prerequisites

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

Procedure

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

2 Right-click the **Roles** tab information panel and click **Add**.

3 Type a name for the new role.

4 Select privileges for the role and click **OK**.

Clone a Role

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

Prerequisites

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

Procedure

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

2 To select the role to duplicate, click the object in the list of **Roles**.

3 To clone the selected role, select **Administration > Role > Clone**.

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

Edit a Role

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

Prerequisites

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

Procedure

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

2 Right-click the role to edit and select **Edit Role**.

3 Select privileges for the role and click **OK**.

Rename a Role

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

Prerequisites

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

Procedure

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

2 Click the object in the list of roles that you want rename.

3 Select **Administration > Role > Rename**.

4 Type the new name.

Remove a Role

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

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

Prerequisites

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

Procedure

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

2 Click the object you want to remove in the list of roles.

3 Select **Administration > Role > Remove**.

4 Click **OK**.

The role is removed from the list.

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

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

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

Using Active Directory to Manage 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.

Configure a Host to Use Active Directory

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

Prerequisites

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

  fully qualified domain name = host_name.domain_name

Procedure

1. Synchronize the time between ESXi and the directory service system using NTP.

   ESXi supports synchronizing time with an external NTPv3 or NTPv4 server that is compliant with RFC 5905 and RFC 1305. The Microsoft Windows W32Time service does not meet these requirements when running with default settings. See the *vSphere Security* documentation or the VMware Knowledge Base for information about how to synchronize ESXi time with a Microsoft Domain Controller.

2. Ensure that the DNS servers you configured for the host can resolve the host names for the Active Directory controllers.

   a. In the vSphere Client, select the host in the inventory.

   b. Click the **Configuration** tab and click **DNS and Routing**.

   c. Click the **Properties** link at the top right of the panel.

   d. In the DNS and Routing Configuration dialog box, verify that the host name and DNS server information for the host are correct.

What to do next

Use the vSphere Client to join a directory service domain.

Add a Host to a Directory Service Domain

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

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

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

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

Prerequisites

Verify that the vSphere Client is connected to the host.

Procedure

1 Select a host in the vSphere Client inventory, and click the **Configuration** tab.

2 Under Software, click **Authentication Services**.

3 Click **Properties**.

4 In the User Directory Services dialog box, select the directory service from the drop-down menu.

5 Enter a domain.

Use the form `name.tld` or `name.tld/container/path`.

6 Click **Join Domain**.

7 Enter the user name and password of a directory service user who has permissions to join the host to the domain, and click **OK**.

8 Click **OK** to close the Directory Services Configuration dialog box.

View Directory Service Settings

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

Procedure

1 Select a host in the vSphere Client inventory, and click the **Configuration** tab.

2 Under Software, select **Authentication Services**.

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

Use vSphere Authentication Proxy to Add a Host to a Domain

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

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

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

Prerequisites

- Verify that the vSphere Client is connected to the host.
- If ESXi is configured with a DHCP address, set up the DHCP range as described in the *vSphere Security* documentation..
- If ESXi is configured with a static IP address, verify that its associated profile is configured to use the vSphere Authentication Proxy service to join a domain so that the authentication proxy server can trust the ESXi IP address.
- If ESXi is using a self-signed certificate, verify that the host has been added to vCenter Server. This allows the authentication proxy server to trust ESXi.

- If ESXi is using a CA-signed certificate and is not provisioned by Auto Deploy, verify that the CA certificate has been added to the local trust certificate store of the authentication proxy server as described in the *vSphere Security* documentation.
- Authenticate the vSphere Authentication Proxy server to the host as described in the *vSphere Security* documentation.

Procedure

1 In the vSphere Client inventory, select the host.

2 Select the **Configuration** tab and click **Authentication Services**.

3 Click **Properties**.

4 In the Directory Services Configuration dialog box, select the directory server from the drop-down menu.

5 Enter a domain.

Use the form `name.tld` or `name.tld/container/path`.

6 Select the **Use vSphere Authentication Proxy** check box.

7 Enter the IP address of the authentication proxy server.

8 Click **Join Domain**.

9 Click **OK**.

Adjust the Search List in Large Domains

If you have domains with thousands of users or groups, or if searches take a long time to complete, adjust the search settings in the Select Users or Groups dialog box.

NOTE This procedure applies only to vCenter Server user lists. ESXi host user lists cannot be searched in the same way.

Prerequisites

To configure Active Directory settings, the vSphere Client must be connected to the vCenter Server system.

Procedure

1 From the vSphere Client connected to a vCenter Server system, select **Administration > vCenter Server Settings**.

2 In the navigation pane, select **Active Directory**.

3 Change the values as needed.

Option	Description
Active Directory Timeout	Timeout interval in seconds for connecting to the Active Directory server. This value specifies the maximum amount of time vCenter Server allows a search to run on the selected domain. Searching large domains can take a long time.
Enable Query Limit	Select the check box to limit the number of users and groups that vCenter Server displays in the Add Permissions dialog box for the selected domain.
Users & Groups value	Specifies the maximum number of users and groups vCenter Server displays from the selected domain in the Select Users or Groups dialog box. If you enter 0 (zero), all users and groups appear.

4 Click **OK**.

Managing Hosts in vCenter Server 8

To access the full capabilities of your hosts and to simplify the management of multiple hosts, you should connect your hosts to a vCenter Server system.

For information about configuration management of ESXihosts, see the *vSphere Networking* documentation, the *vSphere Storage* documentation, or the *vSphere Security* documentation.

The views and capabilities displayed vary depending on whether the vSphere Client is connected to a vCenter Server system or an ESXi host. Unless indicated, the process, task, or description applies to all kinds of vSphere Client connections.

This chapter includes the following topics:

- "Disconnecting and Reconnecting a Host," on page 79
- "Remove a Host from a Cluster," on page 80
- "Remove a Managed Host from vCenter Server," on page 81

Disconnecting and Reconnecting a Host

You can disconnect and reconnect a host that a vCenter Server system manages. Disconnecting a managed host does not remove it from vCenter Server; it temporarily suspends all monitoring activities that vCenter Server performs.

The managed host and its associated virtual machines remain in the vCenter Server inventory. By contrast, removing a managed host from vCenter Server removes the managed host and all its associated virtual machines from the vCenter Server inventory.

Disconnect a Managed Host

Use the vSphere Client to disconnect a managed host from vCenter Server.

Procedure

1. From the vSphere Client connected to a vCenter Server system, display the inventory and click the managed host to disconnect.
2. Right-click the host and select **Disconnect** from the pop-up menu.
3. In the confirmation dialog box that appears, click **Yes**.

   If the managed host is disconnected, the word "disconnected" is appended to the object name in parentheses, and the object is dimmed. All associated virtual machines are similarly dimmed and labeled.

Reconnect a Managed Host

Use the vSphere Client to reconnect a managed host to a vCenter Server system.

Procedure

1 From the vSphere Client connected to a vCenter Server system, display the inventory and click the managed host to reconnect.

2 Right-click the host and select **Connect** from the pop-up menu.

When the managed host's connection status to vCenter Server is changed, the statuses of the virtual machines on that managed host are updated to reflect the change.

Reconnecting Hosts After Changes to the vCenter Server SSL Certificate

vCenter Server uses an SSL certificate to encrypt and decrypt host passwords stored in the vCenter Server database. If the certificate is replaced or changed, vCenter Server cannot decrypt host passwords, and therefore cannot connect to managed hosts.

If vCenter Server fails to decrypt a host password, the host is disconnected from vCenter Server. You must reconnect the host and supply the login credentials, which will be encrypted and stored in the database using the new certificate.

Remove a Host from a Cluster

When a host is removed from a cluster, the resources it provides are deducted from the total cluster resources. The virtual machines deployed on the host are either migrated to other hosts within the cluster, or remain with the host and are removed from the cluster, depending on the state of the virtual machines when the host is removed from the cluster.

You can remove hosts from a cluster by selecting them in the inventory and dragging them to a new location within the inventory. The new location can be a folder as a standalone host or another cluster.

Prerequisites

Before you can remove a host from a cluster, you must power off all virtual machines that are running on the host, or migrate the virtual machines to a new host using vMotion.

Procedure

1 From the vSphere Client connected to a vCenter Server system, display the inventory.

2 Right-click the appropriate managed host icon in the inventory panel, and select **Enter Maintenance Mode** from the pop-up menu.

If all virtual machines on the host are not powered off, the host will not enter maintenance mode.

If the host is inside a DRS-enabled cluster, entering maintenance mode causes DRS to attempt to automatically evacuate powered-on virtual machines from the host using vMotion.

3 In the confirmation dialog that appears, click **Yes**.

The confirmation dialog also asks if you want to automatically evacuate virtual machines that are not powered on from the host. This is useful if you want those virtual machines to remain registered to a host within the cluster.

The host icon changes and the term "maintenance mode" is added to the name in parentheses.

4 Select the host icon in the inventory panel, and drag it to the new location.

   The host can be moved to another cluster or another datacenter. When the new location is selected, a blue box surrounds the cluster or datacenter name.

   vCenter Server moves the host to the new location.

5 Right-click the host, and select **Exit Maintenance Mode** from the pop-up menu.

6 (Optional) Restart any virtual machines, as needed.

Remove a Managed Host from vCenter Server

Remove a managed host from vCenter Server to stop all vCenter Server monitoring and management of that host.

If possible, remove managed hosts while they are connected. Removing a disconnected managed host does not remove the vCenter Server agent from the managed host.

Prerequisites

Make sure NFS mounts are active. If NFS mounts are unresponsive, the operation fails.

Procedure

1 From the vSphere Client connected to a vCenter Server system, display the inventory.

2 (Optional) If the host is part of a cluster, you must put it in maintenance mode.

   a Right-click the managed host in the inventory and select **Enter Maintenance Mode** from the pop-up menu.

   b On the confirmation dialog, click **Yes**.

      The host icon changes and the term “maintenance mode” is added to the name in parentheses.

3 Right-click the appropriate host in the inventory panel, and select **Remove** from the pop-up menu.

4 In the confirmation dialog that appears, click **Yes** to remove the managed host.

   vCenter Server removes the managed host and associated virtual machines from the vCenter Server environment. vCenter Server then returns the status of all associated processor and migration licenses to available.

Using vCenter Maps 9

A vCenter map is a visual representation of your vCenter Server topology. Maps show the relationships between the virtual and physical resources available to vCenter Server.

Maps are available only when the vSphere Client is connected to a vCenter Server system.

The maps can help you determine such things as which clusters or hosts are most densely populated, which networks are most critical, and which storage devices are being utilized. vCenter Server provides the following map views.

Virtual Machine Resources	Displays virtual machine-centric relationships.
Host Resources	Displays host-centric relationships.
Datastore Resources	Displays datastore-centric relationships.
vMotion Resources	Displays hosts available for vMotion migration.

You can use a map view to limit or expand the scope of a map. You can customize all map views, except vMotion Resources maps. If you are accessing map views using the navigation bar, all vCenter Server resources are available for display. If you are using the **Maps** tab of a selected inventory item, only items related to that item are displayed. For virtual machine inventory items, the vMotion Resources view is the only map view available on the **Maps** tab.

You can customize a map view by selecting or deselecting objects in the inventory pane or by selecting or deselecting options in the **Map Relationships** area.

You can reposition the map by dragging it (click and hold anywhere on the map and drag the map to the new location). A grey box in the overview area represents the section of the total map that is viewable and moves as you drag the map. You can resize the grey box to zoom in or out of a section of the map.

You can double-click any object in a map to switch to the **Map** tab for that item (providing a **Map** tab is available for that type of object).

Right-click on any object in a map to access its context menu.

This chapter includes the following topics:

- "Set the Maximum Number of Map Objects," on page 84
- "View vCenter Maps," on page 84
- "Print vCenter Maps," on page 84
- "Export vCenter Maps," on page 84

Set the Maximum Number of Map Objects

In large environments, maps can be slow to load and difficult to read. You can set the maximum number of objects maps can display so that maps load more quickly and are easier to read.

Procedure

1 In the vSphere Client, select **Edit > Client Settings > Maps** tab.

2 Enter the maximum number of objects you want maps to display.

3 Click **OK**.

When a user attempts to view a map that has more objects than the specified limit, the user encounters a message that provides the option to cancel the map or to proceed with displaying it.

View vCenter Maps

Resource maps enable you to view the relationships among hosts, clusters, and virtual machines. You can view a resource map for an entire vCenter Server system or for a specific object, such as a datacenter or cluster. Maps for specific objects show only the object relationships for that object.

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Maps** tab.

For example, to display the resource map for your entire vCenter Server system, select the vCenter Server in the inventory panel. To display the resource map for a host, select the host in the inventory panel.

Print vCenter Maps

You can print resource maps to any standard printer.

Perform this procedure on the vSphere Client **Map** tab.

Procedure

1 Select **File > Print Maps > Print**.

2 In the printer **Name** list, select the printer.

3 Click **Print**.

Export vCenter Maps

Exporting a resource map saves the map to an image file.

Perform this procedure on the vSphere Client **Map** tab.

Procedure

1 If necessary, view the resource map.

2 Select **File > Export > Export Maps**.

3 Navigate to the location to save the file.

4 Type a name for the file and select a file format.

5 Click **Export**.

Creating a Virtual Machine in the vSphere Client 10

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

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

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

This chapter includes the following topics:

- "Start the Virtual Machine Creation Process in the vSphere Client," on page 85
- "Select a Configuration Option for the New Virtual Machine in the vSphere Client," on page 86
- "Enter a Name and Location for the Virtual Machine in the vSphere Client," on page 87
- "Select a Host or Cluster in the vSphere Client," on page 87
- "Select a Resource Pool in the vSphere Client," on page 88
- "Select a Datastore in the vSphere Client," on page 88
- "Select a Virtual Machine Version in the vSphere Client," on page 89
- "Select an Operating System in the vSphere Client," on page 89
- "Select the Number of Virtual CPUs in the vSphere Client," on page 90
- "Configure Virtual Memory in the vSphere Client," on page 90
- "Configure Networks in the vSphere Client," on page 91
- "Select a SCSI Controller in the vSphere Client," on page 92
- "Selecting a Virtual Disk Type," on page 92
- "Complete Virtual Machine Creation in the vSphere Client," on page 96

Start the Virtual Machine Creation Process in the vSphere Client

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

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

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

Prerequisites

Verify that you have the following privileges:

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

Procedure

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

   The New Virtual Machine wizard opens.

What to do next

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

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

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

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

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

Prerequisites

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

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

- Parameters for the virtual disk size and provisioning settings.

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

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

Procedure

1 On the Configuration page of the New Virtual Machine wizard, select an option for creating the virtual machine.

2 Click **Next**.

The Name and Location page appears.

What to do next

Select a name and location for the virtual machine.

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

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

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

Prerequisites

Verify that you have an appropriate naming strategy in place.

Procedure

1 On the Name and Location page of the New Virtual Machine wizard, type a name.

2 Select a folder or the root of the datacenter.

NOTE This option is only available when you are connected to a vCenter Server system.

3 Click **Next**.

The Host / Cluster or the Resource Pool page opens.

Select a Host or Cluster in the vSphere Client

You can place the virtual machine in a cluster or on a host that is not in a cluster.

A cluster is a collection of ESXi hosts and associated virtual machines with shared resources and a shared management interface. Grouping hosts into clusters allows you to enable many optional features that enhance the availability and flexibility of your infrastructure.

Procedure

1 On the Host / Cluster page of the New Virtual Machine wizard, select the host or cluster where you want to run the virtual machine.

NOTE The Host / Cluster page is only available when you are connected to a vCenter Server system.

2 Click **Next**.

If resource pools are configured on the host, the Resource Pool page opens. Otherwise, the Datastore page opens.

What to do next

Select a resource pool or a datastore on which to run the virtual machine.

Select a Resource Pool in the vSphere Client

Resource pools let you manage your computing resources within a host or cluster by setting them up in a meaningful hierarchy. Virtual machines and child resource pools share the resources of the parent resource pool.

The Resource Pool page appears only when resource pools are configured on the host.

Procedure

1 On the Resource Pool page of the New Virtual Machine wizard, navigate to the resource pool where you want to run the virtual machine.

2 Select the resource pool and click **Next.**

The virtual machine is placed in the resource pool you selected.

What to do next

Select a datastore in which to store the virtual machine files.

Select a Datastore in the vSphere Client

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

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

Procedure

1 On the Storage page of the New Virtual Machine wizard, select a datastore in which to store the virtual machine files.

2 (Optional) To turn off Storage DRS for the virtual machine, select **Disable Storage DRS for this virtual machine**.

3 Click **Next**.

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

Select a Virtual Machine Version in the vSphere Client

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

For virtual machine and host compatibility options, see "Virtual Machine Hardware Versions," on page 139.

Procedure

1 Select a virtual machine hardware version.

Option	Description
Virtual machine version 11	Compatible with ESXi 6.0 hosts. Provides the latest virtual machine features including improved accelerated 3D graphics rendering. Recommended for virtual machines that do not need to migrate to ESX/ESXi 4.x and 5.x hosts.
Virtual machine version 10	Compatible with ESXi 5.5 and later hosts. Recommended for virtual machines that do not need to migrate to ESX/ESXi 4.x and 5.1 hosts.
Virtual machine version 9	Compatible with ESXi 5.1 and later hosts. Recommended for virtual machines that do not need to migrate to ESX/ESXi 4.x and 5.0 hosts.
Virtual machine version 8	Compatible with ESXi 5.0 and later hosts. Recommended for virtual machines that do not need to migrate to ESX/ESXi 4.x hosts.
Virtual machine version 7	Compatible with ESX/ESXi 4, 4.x, and later hosts. Recommended for sharing storage or virtual machines with ESX/ESXi versions 3.5 to 4.1.
Virtual machine version 4	Compatible with ESX/ESXi 4 and later hosts. Recommended for virtual machines that need to run on ESX/ESXi versions 4.

2 Click **Next**.

The Guest Operating System page opens.

What to do next

Select a guest operating system for the virtual machine.

Select an Operating System in the vSphere Client

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

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

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

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

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

Procedure

1 On the Guest Operating System page of the New Virtual Machine wizard, select an operating system family.

2 Select an operating system and version from the drop-down menu and click **Next**.

   If any of the total cores available on the host, the maximum virtual CPUs supported by the virtual machine hardware version, or the maximum supported CPUs on the guest operating system equal 1, the virtual machine CPU count is set to 1 and the Memory page opens.

3 If you selected **Other (32-bit)** or **Other (64-bit)**, enter a name for the operating system in the text box.

4 Click **Next**.

What to do next

You can add memory or CPUs for the virtual machine.

Select the Number of Virtual CPUs in the vSphere Client

You can configure a virtual machine to have up to 128 virtual CPUs. The number of licensed CPUs on the host, the number of CPUs that the guest operating system supports, and the virtual machine hardware version determine the number of virtual CPUs that you can add.

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

Procedure

1 On the CPUs page of the New Virtual Machine wizard, select a value from the **Number of virtual sockets** drop-down menu.

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

   To determine the total number of cores, multiply the number of cores per socket by the number of virtual sockets. The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

   The total number of cores appears.

3 Click **Next**.

   The Memory page opens.

What to do next

Select the memory for the virtual machine.

Configure Virtual Memory in the vSphere Client

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

The 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.

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

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

Table 10-1. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Version	Maximum Memory Size
ESXi 6.0	11	4080 GB
ESXi 5.5	10	1011 GB
ESXi 5.1	9	1011 GB
ESXi 5.0	8	1011 GB
ESX/ESXi 4.x	7	255 GB
ESX/ESXi 3.x	4	65,532 MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a version 7 virtual machine that is running on ESXi 5.0 is restricted to 255 GB.

Procedure

1 On the Memory page of the New Virtual Machine wizard, select a size for the virtual memory.

   You can use the slider or use the up and down arrows to select the number. To access the predefined default or recommended setting, click the colored triangles on the right side of the memory bar.

2 Click **Next**.

   The Network page opens.

What to do next

Select network adapters for the virtual machine.

Configure Networks in the vSphere Client

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

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

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

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

Procedure

1 On the Network page of the New Virtual Machine wizard, select the number of NICs to connect from the drop-down menu.

2 For each NIC, select a network and adapter type from the drop-down menus

   Depending on the host version and the guest operating system, a choice of adapter types for each virtual NIC might not be available. In many cases, only one type of adapter is supported. If more than one type of adapter is supported, the recommended type for the guest operating system is selected by default.

3 (Optional) Click **Connect at Power On** to connect the NIC when the virtual machine is powered on.

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

Select a SCSI Controller in the vSphere Client

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

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

LSI Logic SAS and VMware Paravirtual controllers are available only for virtual machines with hardware version 7 or later. For details about VMware Paravirtual controllers, including conditions for use and limitations, see "About VMware Paravirtual SCSI Controllers," on page 166.

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

Procedure

1 On the SCSI Controller page of the New Virtual Machine wizard, accept the default or select a SCSI controller type.

   - BusLogic Parallel
   - LSI Logic Parallel
   - LSI Logic SAS
   - VMware Paravirtual

2 Click **Next**.

   The Select a Disk page opens.

What to do next

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

Selecting a Virtual Disk Type

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

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

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

You can select from the following options:

- Create a Virtual Disk in the vSphere Client on page 93

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

- Use an Existing Virtual Disk in the vSphere Client on page 94

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

- Add an RDM Disk to a Virtual Machine in the vSphere Client on page 95

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

Create a Virtual Disk in the vSphere Client

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

For detailed information about disk types, see the *vSphere Storage* publication.

Procedure

1 On the Create a Disk page of the New Virtual Machine wizard, select the disk size.

  You can increase the disk size later or add disks in the Virtual Machine Properties dialog box.

2 Select the format for the virtual machine's disks and click **Next**.

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

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

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

  The Advanced Options page opens.

4 Accept the default or select a different virtual device node.

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

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

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

6 Click **Next**.

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

What to do next

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

Use an Existing Virtual Disk in the vSphere Client

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

Procedure

1 On the Select Existing Disk page of the New Virtual Machine wizard, browse for a virtual disk file, click **OK**, and click **Next**.

2 Accept the default or select a different virtual device node.

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

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

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

4 Click **Next**.

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

What to do next

Review the virtual machine configuration.

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

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

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

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

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

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

Procedure

1 On the Select a Disk page of the New Virtual Machine wizard, select **Raw Device Mapping** and click **Next**.

2 From the list of SAN disks or LUNs, select a LUN for your virtual machine to access directly and click **Next**.

3 Select a datastore for the LUN mapping file and click **Next**.

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

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

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

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

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

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

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

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

7 Click **Next**.

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

What to do next

Review the virtual machine configuration.

Complete Virtual Machine Creation in the vSphere Client

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

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

Procedure

1 On the Ready to Complete page of the New Virtual Machine wizard, review the configuration settings for the virtual machine.

2 (Optional) Select **Edit the virtual machine settings before completion** and click **Continue**.

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

3 (Optional) Click **Cancel** to go back and review the wizard settings.

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

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

What to do next

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

Working with Templates and Clones in the vSphere Client 11

A clone is a copy of a virtual machine. A template is a master copy of a virtual machine that can be used to create many clones.

When you clone a virtual machine, you create a copy of the entire virtual machine, including its settings, any configured virtual devices, installed software, and other contents of the virtual machine's disks. You also have the option to use guest operating system customization to change some of the properties of the clone, such as the computer name and networking settings.

Cloning a virtual machine can save time if you are deploying many similar virtual machines. You can create, configure, and install software on a single virtual machine, and then clone it multiple times, rather than creating and configuring each virtual machine individually.

If you create a virtual machine that you want to clone frequently, make that virtual machine a template. A template is a master copy of a virtual machine that can be used to create and provision virtual machines. Templates cannot be powered on or edited, and are more difficult to alter than ordinary virtual machine. A template offers a more secure way of preserving a virtual machine configuration that you want to deploy many times.

When you clone a virtual machine or deploy a virtual machine from a template, the resulting cloned virtual machine is independent of the original virtual machine or template. Changes to the original virtual machine or template are not reflected in the cloned virtual machine, and changes to the cloned virtual machine are not reflected in the original virtual machine or template.

This chapter includes the following topics:

- "Clone a Virtual Machine in the vSphere Client," on page 97
- "Create a Scheduled Task to Clone a Virtual Machine in the vSphere Client," on page 100
- "Create a Template in the vSphere Client," on page 100
- "Deploy a Virtual Machine from a Template in the vSphere Client," on page 103
- "Change Template Name in the vSphere Client," on page 105
- "Deleting Templates," on page 106
- "Convert a Template to a Virtual Machine in the vSphere Client," on page 107

Clone a Virtual Machine in the vSphere Client

Cloning a virtual machine creates a duplicate of the virtual machine with the same configuration and installed software as the original.

Optionally, you can customize the guest operating system of the clone to change the virtual machine name, network settings, and other properties. This prevents conflicts that can occur if a virtual machine and a clone with identical guest operating system settings are deployed simultaneously.

Prerequisites

- You must be connected to vCenter Server in order to clone a virtual machine. You cannot clone virtual machines if you connect directly to an ESXi host.
- To customize the guest operating system of the virtual machine, check that your guest operating system meets the requirements for customization. See "Guest Operating System Customization Requirements," on page 109.
- To use a customization specification, you must first create or import the customization specification.
- To use a custom script to generate the host name or IP address for the new virtual machine, configure the script. See "Configure a Script to Generate Computer Names and IP Addresses During Guest Operating System Customization in the vSphere Client," on page 110.

Procedure

1. Right-click the virtual machine and select **Clone**.
2. Enter a virtual machine name, select a location, and click **Next**.
3. Select a host or cluster on which to run the new virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click **Next**. b Select a host within the cluster and click **Next**.

4. Select a resource pool in which to run the virtual machine and click **Next**.
5. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store virtual machine configuration files and disk in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c Click **Next**.

6 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
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 thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

7 Select a guest operating system customization option.

Option	Description
Do not customize	Select **Do not customize** and click **Next**. Does not customize any of the guest operating system settings. All settings remain identical to those of the source virtual machine.
Customize using the Customization Wizard	Opens the Customization Wizard so that you can select customization options for the guest operating system. Select this option and click **Next** to launch the Customization Wizard. ■ To customize a Linux guest operating system, see "Customize Linux During Cloning or Deployment in the vSphere Client," on page 113. ■ To customize a Windows guest operating system, see "Customize Windows During Cloning or Deployment in the vSphere Client," on page 111.
Customize using an existing customization specification	Uses the settings in a saved customization specification to customize the guest operating system. a Select **Customize using an existing customization specification**. b Select the customization specification that you want to use. c (Optional) Select **Use the Customization Wizard to temporarily adjust the specification before deployment** if you want to make changes to the specification for this deployment only. d Click **Next**.

8 Review your selections and select whether to power on the virtual machine or edit virtual machine settings.

Option	Action
Power on this virtual machine after creation.	Select this option and click **Finish**. The virtual machine powers on after the deployment task completes.
Edit virtual hardware.	a Select this option and click **Continue**. b Make any changes and click **OK**.

The cloned virtual machine is deployed. You cannot use or edit the virtual machine until the cloning is complete. This might take several minutes if the cloning involves creating a virtual disk. You can cancel the cloning at any point before the customization stage.

Create a Scheduled Task to Clone a Virtual Machine in the vSphere Client

This procedure creates a scheduled task to clone a virtual machine.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.

Procedure

1. From the Home page, click **Scheduled Tasks**.
2. Select **File > New > Scheduled Task**, or click **New**.

   The **Select a Task to Schedule** dialog box appears.
3. Select **Clone a virtual machine** from the drop-down menu, and click **OK**.

   The Clone Virtual Machine wizard appears.
4. Select the virtual machine to clone and click **Next**.
5. Follow the wizard through the same steps as those in the previous task in which you cloned a virtual machine.
6. Enter a name and a task description in the text box.
7. Select the frequency of the task.
8. Select **Now** or **Later**. If later, enter the time and date when you want the virtual machine to be deployed, and click **Next**.

   To see the calendar, click **Later**, and click the drop-down arrow to select a date from the calendar. A red circle indicates today's date, and a dark circle indicates the scheduled date.
9. Review the information on the Ready to Complete New Virtual Machine page, and click **Finish**.

   Optionally, you can select the check box to power on the new virtual machine after it is created.

   vCenter Server adds the new task to the scheduled task list and completes it at the designated time. When it is time to perform the task, vCenter Server first verifies that the user who created the task still has permission to complete the task. If the permission levels are not acceptable, vCenter Server sends a message to the log and the task is not performed.

Create a Template in the vSphere Client

Create a template to create a master image of a virtual machine from which you can deploy many virtual machines.

You can create a template by converting a virtual machine to a template, cloning a virtual machine to a template, or cloning another template.

Convert a Virtual Machine to a Template in the vSphere Client

You can convert a virtual machine directly to a template instead of making a copy by cloning.

When you convert a virtual machine to a template, you cannot edit or power on the template unless you convert it back to a virtual machine.

Prerequisites

- You must be connected to vCenter Server to convert a virtual machine to a template. You cannot create templates if you connect the vSphere Client directly to an ESXi host.

- Before you convert a virtual machine to a template, select it in the inventory and power it off.

Procedure

◆ Right-click the virtual machine and select **Template > Convert to Template**.

vCenter Server marks that virtual machine as a template and displays the task in the Recent Tasks pane.

Clone Virtual Machine to Template in the vSphere Client

Cloning a virtual machine to a template creates a template copy of the virtual machine while leaving the original virtual machine in place.

Prerequisites

You must be connected to vCenter Server to clone a virtual machine to a template. You cannot create templates if you connect directly to an ESXi host.

Procedure

1 Right-click the virtual machine and select **Template > Clone to Template**.

2 Give the new template a name, select its inventory location, and click **Next**.

3 Pass through the target location page and click **Next**.

4 Specify in which format to store the template's virtual disks and click **Next**.

Option	Action
Same format as source	Use the same format as the source virtual machine.
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 thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

5 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store virtual machine configuration files and disk in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c Click **Next**.

6 Click **Finish**.

vCenter Server displays the Tasks inventory panel for reference and adds the cloned template to the list in the information panel.

Clone a Template in the vSphere Client

Clone a template to create a copy of it.

Prerequisites

You must be connected to vCenter Server to clone a template. You cannot create templates if you connect directly to an ESXi host.

Procedure

1 Right-click the template and select **Clone**.

2 Give the new template a unique name and description and click **Next**.

3 Select the host or cluster and click **Next**.

4 Select a datastore for the template and click **Next**.

5 Specify in which format to store the template's virtual disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
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.

Option	Action
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 thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

6 Click **Next**.

7 Review the information for the template and click **Finish**.

You cannot use the new template until the cloning task completes.

vCenter Server adds the cloned template to the list in the **Virtual Machines** tab.

Deploy a Virtual Machine from a Template in the vSphere Client

Deploying a virtual machine from a template creates a new virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties configured for the template.

Prerequisites

- Verify that you are connected to vCenter Server. You cannot work with templates if you connect the vSphere Client directly to an ESXi host.
- You must be connected to vCenter Server to deploy a virtual machine from a template. You cannot deploy from a template if you connect the vSphere Client directly to an ESXi host.
- To customize the guest operating system of the virtual machine, check that your guest operating system meets the requirements for customization. See "Guest Operating System Customization Requirements," on page 109.
- To use a customization specification, create or import the customization specification.
- To use a custom script to generate the host name or IP address for the new virtual machine, configure the script. See "Configure a Script to Generate Computer Names and IP Addresses During Guest Operating System Customization in the vSphere Client," on page 110.

Procedure

1 Right-click the template, and select **Deploy Virtual Machine from this Template**.

2 Enter a virtual machine name, select a location, and click **Next**.

3 Select a host or cluster on which to run the new virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click **Next**. b Select a host within the cluster and click **Next**.

4 Select a resource pool in which to run the virtual machine and click **Next**.

5 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. b Select a datastore cluster. c (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. d Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c (Optional) Apply a virtual machine storage policy from the **VM storage profile** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. d (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. e Click **Next**.

6 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
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 thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

7 Select a guest operating system customization option.

Option	Description
Do not customize	Select **Do not customize** and click **Next**. Does not customize any of the guest operating system settings. All settings remain identical to those of the source virtual machine.
Customize using the Customization Wizard	Opens the Customization Wizard so that you can select customization options for the guest operating system. Select this option and click **Next** to launch the Customization Wizard. ■ To customize a Linux guest operating system, see "Customize Linux During Cloning or Deployment in the vSphere Client," on page 113. ■ To customize a Windows guest operating system, see "Customize Windows During Cloning or Deployment in the vSphere Client," on page 111.
Customize using an existing customization specification	Uses the settings in a saved customization specification to customize the guest operating system. a Select **Customize using an existing customization specification**. b Select the customization specification that you want to use. c (Optional) Select **Use the Customization Wizard to temporarily adjust the specification before deployment** if you want to make changes to the specification for this deployment only. d Click **Next**.

8 Review your selections and select whether to power on the virtual machine or edit virtual machine settings.

Option	Action
Power on this virtual machine after creation	Select this option and click **Finish**. The virtual machine powers on after the deployment task completes.
Edit virtual hardware	a Select this option and click **Continue**. b Make any changes and click **OK**.
Show all storage recommendations	This option appears only when the virtual machine disks are stored on a datastore cluster and Storage DRS is enabled. Select this option, and click **Continue**. The dialog box lists the datastores in the datastore cluster that are recommended for virtual machine placement.
Edit Storage DRS rules	This option appears only when the virtual machine disks are stored on a datastore cluster. This option is selected when you select **Edit virtual hardware**. You can edit Storage DRS rules on the **Options** tab of the Virtual Machine Properties dialog box. Select the **Edit Storage DRS rules** check box, and click **Continue**.

The virtual machine is deployed. You cannot use or edit the virtual machine until the deployment is complete. This might take several minutes if the deployment involves creating a virtual disk.

Change Template Name in the vSphere Client

Unlike other changes to templates, you do not have to convert a template to a virtual machine to change the name of a template.

Prerequisites

Verify that you are connected to vCenter Server. You cannot work with templates if you connect the vSphere Client directly to an ESXi host.

Procedure

1 Right-click the template and select **Rename**.

2 Enter a new name and click outside the field to save your changes.

Deleting Templates

You can delete a template by removing it from the inventory or deleting the template from the disk. If you remove the template from the inventory, it remains on the disk and can be reregistered with vCenter Server to restore it to the inventory.

- Remove Templates from the Inventory in the vSphere Client on page 106

  If you remove a template from the inventory, it is unregistered from the vCenter Server inventory, but it is not removed from the datastore.

- Delete a Template from the Disk in the vSphere Client on page 106

  Deleted templates are permanently removed from the system.

- Reregister Templates in the vSphere Client on page 107

  Templates can become unregistered from the vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from the vCenter Server and then readded.

Remove Templates from the Inventory in the vSphere Client

If you remove a template from the inventory, it is unregistered from the vCenter Server inventory, but it is not removed from the datastore.

Prerequisites

You must be connected to vCenter Server to remove a template from the inventory. You cannot work with templates if you connect directly to an ESXi host.

Procedure

1 Right-click the template, and select **Remove from Inventory**.

2 Click **OK** to confirm removing the template from the vCenter Server database.

  The template is unregistered from the vCenter Server inventory.

Delete a Template from the Disk in the vSphere Client

Deleted templates are permanently removed from the system.

Prerequisites

You must be connected to vCenter Server to delete a template. You cannot work with templates if you connect the vSphere Client directly to an ESXi host.

Procedure

1 Right-click the template, and select **Delete from Disk**.

2 Click **OK** to confirm removing the template from the datastore.

  The template is deleted from the disk and cannot be recovered.

Reregister Templates in the vSphere Client

Templates can become unregistered from the vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from the vCenter Server and then readded.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.

Procedure

1. From the Home page, click **Datastores and Datastore Clusters**.
2. Right-click the datastore that contains the template and select **Browse Datastore**.
3. Browse through the datastore folders to find the `.vmtx` file.
4. Right-click the `.vmtx` file and select **Add to Inventory**.

   The Add to Inventory wizard appears.
5. Enter a template machine name, select a location, and click **Next**.

   If you want the template to retain its original name, do not enter a name in the Add to Inventory wizard. vCenter Server will use the original name if the field in the wizard is left blank.
6. Select a host or cluster on which to store the template, and click **Next**.
7. Review your selections, and click **Finish**.

The template is registered to the host. You can view the template from the host's **Virtual Machine** tab.

Convert a Template to a Virtual Machine in the vSphere Client

Converting a template to a virtual machine changes the template rather than making a copy. You can convert a template to a virtual machine to edit the template. You might also convert a template to a virtual machine if you no longer need to preserve it as a master image for deploying virtual machines.

Prerequisites

You must be connected to vCenter Server to convert a template to a virtual machine. You cannot work with templates if you connect directly to an ESXi host.

Procedure

1. Right-click the template and select **Convert to Virtual Machine**.
2. Select the host or cluster on which to run the virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click **Next**. b Select a host within the cluster and click **Next**.

   If the template resides on a legacy VMFS2 datastore, you must select the host on which the template was created as the destination for the virtual machine.
3. Select a resource pool in which to run the virtual machine and click **Next**.
4. Review your selections and click **Finish**.

Customizing Guest Operating Systems 12

When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings.

Customizing guest operating systems can help prevent conflicts that can result if virtual machines with identical settings are deployed, such as conflicts due to duplicate computer names.

You can specify the customization settings by choosing to launch the Guest Customization wizard during the cloning or deployment process. Alternatively, you can create customization specifications, which are customization settings stored in the vCenter Server database. During the cloning or deployment process, you can select a customization specification to apply to the new virtual machine.

Use the Customization Specification Manager to manage customization specifications you create with the Guest Customization wizard.

This chapter includes the following topics:

- "Guest Operating System Customization Requirements," on page 109
- "Configure a Script to Generate Computer Names and IP Addresses During Guest Operating System Customization in the vSphere Client," on page 110
- "Customize Windows During Cloning or Deployment in the vSphere Client," on page 111
- "Customize Linux During Cloning or Deployment in the vSphere Client," on page 113
- "Managing Customization Specifications in the vSphere Client," on page 115

Guest Operating System Customization Requirements

To customize the guest operating system, you must configure the virtual machine and guest to meet VMware Tools and virtual disk requirements. Other requirements apply, depending on the guest operating system type.

VMware Tools Requirements

The current version of VMware Tools must be installed on the virtual machine or template to customize the guest operating system during cloning or deployment.

Virtual Disk Requirements

The guest operating system being customized must be installed on a disk attached as SCSI node 0:0 in the virtual machine configuration.

Windows Requirements

Customization of Windows guest operating systems requires the following conditions:

- Microsoft Sysprep tools must be installed on the vCenter Server system.
- The ESXi host that the virtual machine is running on must be 3.5 or later.

Guest operating system customization is supported on multiple Windows operating systems.

Linux Requirements

Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system.

Guest operating system customization is supported on multiple Linux distributions.

Verifying Customization Support for a Guest Operating System

To verify customization support for Windows operating systems or Linux distributions and compatible ESXi hosts, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility. You can use this online tool to search for the guest operating system and ESXi version. After the tool generates your list, click the guest operating system to see whether guest customization is supported.

Configure a Script to Generate Computer Names and IP Addresses During Guest Operating System Customization in the vSphere Client

As an alternative to entering the computer name or IP addresses for virtual NICs during guest operating system customization, you can create a custom application and configure it so that vCenter Server can use it to generate the computer name and IP addresses.

The application can be an arbitrary executable binary or script file appropriate for the corresponding operating system in which vCenter Server is running. After you configure a name-ip-generation application in vCenter Server, each time you initiate a guest os customization for a virtual machine, the name-ip-app is executed and an XML string is generated in place and passed to its standard input. The name-ip-generation application on its behalf should generate and return the resulting XML string through its standard output.

The application must comply with the reference XML file in the VMware knowledge base article at http://kb.vmware.com/kb/2007557.

Prerequisites

Verify that Perl is installed on vCenter Server.

Procedure

1. Create the script and save it on the vCenter Server system's local disk.
2. In the vSphere Client connected to vCenter Server, select **Administration > vCenter Server Settings**.
3. Select **Advanced Settings**.
4. Enter the configuration parameters for the script.
   a. In the **Key** text box, type **`config.guestcust.name-ip-generator.arg1`**.
   b. In the **Value** text box, type **`c:\sample-generate-name-ip.pl`** and click **Add**.
   c. In the **Key** text box, type **`config.guestcust.name-ip-generator.arg2`**.
   d. In the **Value** text box, type the path to the script file on the vCenter Server system and click **Add**. For example, type `c:\sample-generate-name-ip.pl`.

e In the **Key** text box, type `config.guestcust.name-ip-generator.program`.

f In the **Value** text box, type `c:\perl\bin\perl.exe` and click **Add**.

5 Click **OK**.

You can select the option to use an application to generate computer names or IP addresses during customization.

Customize Windows During Cloning or Deployment in the vSphere Client

When you deploy a new virtual machine from a template or clone an existing virtual machine, you can customize Windows guest operating systems for the virtual machine.

NOTE The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine boots the first time after customization.

Prerequisites

Verify that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 109.

Procedure

1 Select **View > Management > Customization Management Manager** and click **New** to start the Windows Guest Customization.

2 Select the **Target Virtual Machine OS** and enter the name and description for the Customization Specification Information, then click **Next**.

NOTE If you want to use a custom sysprep file, select **Use Custom Sysprep Answer File**.

---

3 Type the virtual machine owner's name and organization and click **Next**.

4 Enter the guest operating system's computer name and click **Next**.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.

Option	Action
Enter a name in the Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

5 Provide licensing information for the Windows operating system and click **Next**.

Option	Action
For non-server operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	a Type the Windows product key for the new guest operating system. b Select **Include Server License Information**. c Select either **Per seat** or **Per server**. d (Optional) If you select **Per server**, enter the maximum number of simultaneous connections for the server to accept.

6 Configure the administrator password for the virtual machine and click **Next**.

a Type a password for the administrator account and confirm the password by typing it again.

NOTE You can change the administrator password only if the administrator password on the source Windows virtual machine is blank. If the source Windows virtual machine or template already has a password, the administrator password does not change.

b (Optional) To log users into the guest operating system as Administrator, select the check box, and select the number of times to log in automatically.

7 Select the time zone for the virtual machine and click **Next**.

8 (Optional) On the Run Once page, specify commands to run the first time a user logs into the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about `RunOnce` commands.

9 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

10 Select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, `MSHOME`.
Windows Server Domain	a Type the domain name. b Type the user name and password for a user account that has permission to add a computer to the specified domain.

11 (Optional) Select Generate New Security ID (SID) and click **Next**.

   A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

   Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

12 Save the customized options as an `.xml` file.

   a Select **Save this customization specification for later use**.

   b Specify the filename for the specification and click **Next**.

13 Click **Finish** to save your changes.

You return to the Deploy Template or to the Clone Virtual Machine wizard. The customization is finished after you complete the Deploy Template or the Clone Virtual Machine wizard.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

After you deploy and customize versions of Windows XP or Windows 2003 that are not volume licensed, you might need to reactivate your operating system on the new virtual machine.

If the new virtual machine encounters customization errors while it is booting, the errors are logged to `%WINDIR%\temp\vmware-imc`. To view the error log file, click the Windows **Start** button and select **Programs > Administrative Tools > Event Viewer**.

Customize Linux During Cloning or Deployment in the vSphere Client

In the process of deploying a new virtual machine from a template or cloning an existing virtual machine, you can customize Linux guest operating systems for the virtual machine.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 109.

Procedure

1 Select **View > Management > Customization Management Manager** and click **New** to start the Windows Guest Customization.

2 Select the **Target Virtual Machine OS** and enter the name and description for the Customization Specification Information, then click **Next**.

   NOTE If you want to use a custom sysprep file, select **Use Custom Sysprep Answer File**.

3 Select **Customize using the Customization Wizard** and click **Next**.

4 Specify how to determine the host name to identify the guest operating system on the network.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.
Enter a name in the Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

5 Enter the **Domain Name** for the computer and click **Next**.

6 Select the time zone for the virtual machine and click **Next**.

7 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

8 Enter DNS and domain settings.

9 Save the customized options as an `.xml` file.

   a Select **Save this customization specification for later use**.

   b Specify the filename for the specification and click **Next**.

10 Click **Finish** to save your changes.

You return to the Deploy Template or to the Clone Virtual Machine wizard. The customization is finished after you complete the Deploy Template or the Clone Virtual Machine wizard.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

If the new virtual machine encounters customization errors while it is booting, the errors are reported using the guest's system logging mechanism. View the errors by opening `/var/log/vmware-imc/toolsDeployPkg.log`.

Managing Customization Specifications in the vSphere Client

Customization specifications are XML files that contain guest operating system settings for virtual machines. You create customization specifications with the Guest Customization wizard, and manage specifications using the Customization Specification Manager.

vCenter Server saves the customized configuration parameters in the vCenter Server database. If the customization settings are saved, the administrator, and domain administrator, passwords are stored in encrypted format in the database. Because the certificate used to encrypt the passwords is unique to each vCenter Server system, reinstalling vCenter Server, or attaching a new instance of the server the database, invalidates the encrypted passwords. The passwords must be re-entered before they can be used.

Create a Customization Specification for Linux in the vSphere Client

Use the Guest Customization wizard to save guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 109.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Click the **Create New Specification** icon.

3 Select Linux from the **Target Virtual Machine OS** menu.

4 Under Customization Specification Information, enter a name for the specification and an optional description and click **Next**.

5 Specify how to determine the host name to identify the guest operating system on the network.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.
Enter a name in the Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

6 Enter the **Domain Name** for the computer and click **Next**.

7 Select the time zone for the virtual machine and click **Next**.

8 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

9 Enter DNS and domain settings.

10 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows in the vSphere Client

Use the Guest Customization wizard to save Windows guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

NOTE The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine boots the first time after customization.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 109.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Click the **Create New Specification** icon.

3 In the Guest Customization wizard, select Windows from the **Target Virtual Machine OS** menu.

4 Under Customization Specification Information, enter a name for the specification and an optional description and click **Next**.

5 Type the virtual machine owner's name and organization and click **Next**.

6 Enter the guest operating system's computer name and click **Next**.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.
Enter a name in the Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

7 Provide licensing information for the Windows operating system and click **Next**.

Option	Action
For non-server operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	a Type the Windows product key for the new guest operating system. b Select **Include Server License Information**. c Select either **Per seat** or **Per server**. d (Optional) If you select **Per server**, enter the maximum number of simultaneous connections for the server to accept.

8 Configure the administrator password for the virtual machine and click **Next**.

a Type a password for the administrator account and confirm the password by typing it again.

Note You can change the administrator password only if the administrator password on the source Windows virtual machine is blank. If the source Windows virtual machine or template already has a password, the administrator password does not change.

b (Optional) To log users into the guest operating system as Administrator, select the check box, and select the number of times to log in automatically.

9 Select the time zone for the virtual machine and click **Next**.

10 (Optional) On the Run Once page, specify commands to run the first time a user logs into the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about `RunOnce` commands.

11 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

12 Select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, `MSHOME`.
Windows Server Domain	a Type the domain name. b Type the user name and password for a user account that has permission to add a computer to the specified domain.

13 (Optional) Select Generate New Security ID (SID) and click **Next**.

A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

14 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows Using a Custom Sysprep Answer File in the vSphere Client

A custom sysprep answer file is a file that stores a number of customization settings such as computer name, licensing information, and workgroup or domain settings. You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the Guest Customization wizard.

Windows 2000, Windows Server 2003, and Windows XP use a text file called `sysprep.inf`. Windows Server 2008, Windows Vista, and Windows 7 use an XML file called `sysprep.xml`. You can create these files using a text editor, or use the Microsoft Setup Manager utility to generate them. For more information about how to create a custom sysprep answer file, see the documentation for the relevant operating system.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 109.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Click the **Create New Specification** icon.

3 In the Guest Customization wizard, select Windows from the **Target Virtual Machine OS** menu.

4 (Optional) Select **Use Custom Sysprep Answer File**.

5 Under Customization Specification Information, enter a name for the specification and an optional description and click **Next**.

6 Select the option to import or create a sysprep answer file and click **Next**.

Option	Description
Import a Sysprep answer file	Click **Browse** and browse to the file.
Create a Sysprep answer file	Type the contents of the file in the text box.

7 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

8 (Optional) Select Generate New Security ID (SID) and click **Next**.

A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

9 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Edit a Customization Specification in the vSphere Client

You can edit existing specifications using the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Right-click a specification and select **Edit**.

3 Proceed through the Guest Customization wizard to change specification settings.

Remove a Customization Specification in the vSphere Client

You can remove customization specifications from the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Right-click a specification and select **Remove**.

3 In the confirmation dialog box, select **Yes**.

The specification is deleted from the disk.

Copy a Customization Specification in the vSphere Client

You can copy an existing customization specification using the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Right-click a specification and select **Copy**.

A new specification is created, Copy of *specification_name*.

Export a Customization Specification in the vSphere Client

You can export customization specifications and save them as `.xml` files. To apply an exported specification to a virtual machine, import the .xml file using the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Right-click a specification and select **Export**.

3 In the **Save As** dialog, enter a file name and location.

4 Click **Save**.

The specification is saved as an `.xml` file to the location you specified.

Import a Customization Specification in the vSphere Client

You can import an existing specification using the Customization Specification Manager, and use the specification to customize the guest operating system of a virtual machine.

Prerequisites

Before you begin, you must have at least one customization specification saved as an xml file located on a file system accessible from the vSphere Client.

Procedure

1 From the vSphere Client Home page, select **Customization Specifications Manager**.

2 Click **Import**.

3 From the Open dialog, browse to the `.xml` to import and click **Open**.

The imported specification is added to the list of customization specifications.

Migrating Virtual Machines in the vSphere Client

13

You can move virtual machines from one host or storage location to another location using hot or cold migration. For example, with vMotion you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to collocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

You can use cold or hot migration to move virtual machines to different hosts or datastores.

Cold Migration

You can move a powered off or suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one datacenter to another. To perform a cold migration, you can move virtual machines manually or set up a scheduled task.

Hot Migration

Depending on the type of migration you are using, vMotion or Storage vMotion, you can move a turned on virtual machine to a different host, or move its disks or folder to a different datastore without any interruption in the availability of the virtual machine. vMotion is also referred to as live migration or hot migration.

You cannot move a powered on virtual machine from one datacenter to another.

NOTE Copying a virtual machine creates a new virtual machine. It is not a form of migration. Cloning a virtual machine or copying its disks and configuration file creates a new virtual machine. Cloning is not a form of migration.

In vCenter Server, you have the following migration options:

Change Host Moving a virtual machine, but not its storage to another host. You can move the virtual machine using cold migration or hot migration. You use vMotion to move a powered on virtual machine to another host.

Change Datastore Moving a virtual machine and its storage, including virtual disks and configuration files or a combination of these, to a new datastore on the same host. You can change the datastore using cold or hot migration. You use Storage Migration to move a powered on virtual machine and its storage to a new datastore.

Change Host and Datastore Moving a virtual machine to another host and moving its disk or virtual machine folder to another datastore. You can change the host and datastore using cold or hot migration. Hot migration is a combination of Storage vMotion and vMotion.

To migrate virtual machines with disks larger than 2TB, the source and destination hosts must run ESXi 5.5 or later.

This chapter includes the following topics:

- "Migrate a Powered-On Virtual Machine with vMotion in the vSphere Client," on page 124
- "Migrate a Virtual Machine with Storage vMotion in the vSphere Client," on page 125
- "Migrate a Powered-Off or Suspended Virtual Machine in the vSphere Client," on page 126
- "CPU Compatibility and EVC," on page 128

Migrate a Powered-On Virtual Machine with vMotion in the vSphere Client

You can use the Migration wizard to migrate a powered-on virtual machine from one host to another using vMotion technology. To relocate the disks of a powered-on virtual machine, migrate the virtual machine using Storage vMotion.

Prerequisites

Before migrating a virtual machine with vMotion, ensure that your hosts and virtual machines meet the requirements for migration with vMotion. See the *vCenter Server and Host Management* publication for more information on host configuration and VM conditions and limitations for vMotion.

Procedure

1 Select the virtual machine that you want to migrate in the inventory.

2 Right-click on the virtual machine and select **Migrate** from the pop-up menu.

3 Select **Change host** and click **Next**.

4 Select a destination host or cluster for the virtual machine.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and fully automated DRS clusters. You can select a non-automated cluster as a target. You are prompted to select a host within the non-automated cluster.

5 Select a resource pool and click **Next**.

6 Select the migration priority level and click **Next**.

Option	Description
High Priority	On hosts running ESX/ESXi version 4.1 or later, vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources to high priority migrations than to standard priority migrations. Migrations always proceed regardless of the resources that have been reserved. On hosts running ESX/ESXi version 4.0 or earlier, vCenter Server attempts to reserve a fixed amount of resources on both the source and destination hosts for each migration. High priority migrations do not proceed if resources are unavailable.
Standard Priority	On hosts running ESX/ESXi version 4.1 or later, vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources to standard priority migrations than to high priority migrations. Migrations always proceed regardless of the resources that have been reserved. On hosts running ESX/ESXi version 4.0 or earlier, vCenter Server attempts to reserve a fixed amount resources on the source and destination hosts for each migration. Standard priority migrations always proceed. However, the migration might proceed more slowly or fail to complete if sufficient resources are not available.

7 Review the page and click **Finish**.

A task is created that begins the virtual machine migration process.

Migrate a Virtual Machine with Storage vMotion in the vSphere Client

Use migration with Storage vMotion to relocate a virtual machine's configuration file and virtual disks while the virtual machine is powered on.

You cannot change the virtual machine's execution host during a migration with Storage vMotion.

Procedure

1 Select the virtual machine that you want to migrate in the inventory.

2 Right-click on the virtual machine and select **Migrate** from the pop-up menu.

3 Select **Change datastore** and click **Next**.

4 Select a disk format.

Option	Description
Same as Source	Use the format of the original virtual disk.
Thin provisioned	Use the thin format to save storage space. The thin virtual disk uses just as much storage space as it needs for its initial operations. When the virtual disk requires more space, it can expand up to its maximum allocated capacity.
Thick	Allocate a fixed amount of hard disk space to the virtual disk. The virtual disk in the thick format does not change its size and from the beginning occupies the entire datastore space provisioned to it.

5 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store virtual machine configuration files and disk in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c Click **Next**.

6 Review the page and click **Finish**.

Migrate a Powered-Off or Suspended Virtual Machine in the vSphere Client

You can use the Migration wizard to migrate a powered-off virtual machine or suspended virtual machine.

Procedure

1 Right-click the virtual machine and select **Migrate**.

   a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.
Migrate virtual machine(s) to a specific datacenter	Move the virtual machine to a virtual data center, where you can assign policies to VMs.

3 To move the virtual machine to another host, select the destination host or cluster for this virtual machine migration and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster itself.

4 Select the destination resource for the virtual machine migration.

5 If you chose to move the configuration file and virtual disks of the virtual machine, select a disk format.

Option	Description
Same as Source	Use the format of the original virtual disk.
Thin provisioned	Use the thin format to save storage space. The thin virtual disk uses just as much storage space as it needs for its initial operations. When the virtual disk requires more space, it can expand up to its maximum allocated capacity.
Thick	Allocate a fixed amount of hard disk space to the virtual disk. The virtual disk in the thick format does not change its size and from the beginning occupies the entire datastore space provisioned to it.

Disks are converted from thin to thick format or thick to thin format only when they are copied from one datastore to another. If you leave a disk in its original location, the disk format is not converted, regardless of the selection made here.

6 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. b Select a datastore cluster. c (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. d Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c (Optional) Apply a virtual machine storage policy from the **VM storage profile** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. d (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. e Click **Next**.

7 Review the page and click **Finish**.

vCenter Server moves the virtual machine to the new host. Event messages appear in the **Events** tab. The data displayed on the Summary tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

CPU Compatibility and EVC

vCenter Server performs compatibility checks before it allows migration of running or suspended virtual machines to ensure that the virtual machine is compatible with the target host.

vMotion transfers the running state of a virtual machine between underlying ESXi systems. Live migration requires that the processors of the target host provide the same instructions to the virtual machine after migration that the processors of the source host provided before migration. Clock speed, cache size, and number of cores can differ between source and target processors. However, the processors must come from the same vendor class (AMD or Intel) to be vMotion compatible.

NOTE Do not add virtual ESXi hosts to an EVC cluster. ESXi virtual machines are not supported in EVC clusters.

Migrations of suspended virtual machines also require that the virtual machine be able to resume execution on the target host using equivalent instructions.

When you initiate a migration with vMotion or a migration of a suspended virtual machine, the Migrate Virtual Machine wizard checks the destination host for compatibility and produces an error message if compatibility problems will prevent migration.

The CPU instruction set available to the operating system and to applications running in a virtual machine is determined at the time that a virtual machine is powered on. This CPU feature set is based on the following items:

- Host CPU family and model
- Settings in the BIOS that might disable CPU features
- ESX/ESXi version running on the host
- The virtual machine's compatibility setting
- The virtual machine's guest operating system

To improve CPU compatibility between hosts of varying CPU feature sets, some host CPU features can be hidden from the virtual machine by placing the host in an Enhanced vMotion Compatibility (EVC) cluster.

NOTE You can hide Host CPU features from a virtual machine by applying a custom CPU compatibility mask to the virtual machine, but this is not recommended. VMware, in partnership with CPU and hardware vendors, is working to maintain vMotion compatibility across the widest range of processors. For additional information, search the VMware Knowledge Base for the *vMotion and CPU Compatibility FAQ*.

Create an EVC Cluster

Create an EVC cluster to help ensure vMotion compatibility between the hosts in the cluster.

When you create an EVC cluster, use one of the following methods:

- Create an empty cluster, enable EVC, and move hosts into the cluster.
- Enable EVC on an existing cluster.

VMware recommends creating an empty EVC cluster as the simplest way of creating an EVC cluster with minimal disruption to your existing infrastructure.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.
- Before you create an EVC cluster, ensure that the hosts you intend to add to the cluster meet the requirements listed in the *vCenter Server and Host Management* publication.

Procedure

1 In the vSphere Client, right-click on a data center and click **New Cluster**.

2 Enter a name for the cluster and select cluster features, then click **Next**.

   Cluster features such as vSphere DRS and vSphere HA are fully compatible with EVC. You can enable these features when you create the cluster. For information on specific cluster options, see the vSphere Client online Help.

3 Select the CPU vendor and EVC mode appropriate for the hosts you intend to add to the cluster and click **Next**.

4 Select the Swapfile Policy and click **Next**.

5 Review the selected options for the cluster and click **Finish** to create the cluster.

6 Select a host from the inventory to move into the cluster.

7 If the host feature set is greater than the EVC mode that you have enabled for the EVC cluster, ensure that the cluster has no powered-on virtual machines.

   - Power off all the virtual machines on the host.
   - Migrate the host's virtual machines to another host using vMotion.

8 Move the host into the cluster.

   You can power on the virtual machines on the host, or migrate virtual machines into the cluster with vMotion, if the virtual machines meet CPU compatibility requirements for the cluster's EVC mode. Virtual machines running on hosts with more features than the EVC mode must be powered off before migration into the cluster.

9 Repeat Step 7 and Step 8 for each additional host that you want to move into the cluster.

Enable EVC on an Existing Cluster

Enable EVC on an existing cluster to help ensure vMotion compatibility between the hosts in the cluster.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.
- Before you enable EVC on an existing cluster, ensure that the hosts in the cluster meet the requirements listed in the *vCenter Server and Host Management* publication.

Procedure

1 In the vSphere Client, select the cluster for which you want to enable EVC.

2 If virtual machines are running on hosts that have feature sets greater than the EVC mode you intend to enable, ensure that the cluster has no powered-on virtual machines.

   - Power off all the virtual machines on the hosts with feature sets greater than the EVC mode
   - Migrate the cluster's virtual machines to another host using vMotion.

     Because these virtual machines are running with more features than the EVC mode you intend to set, power off the virtual machines to migrate them back into the cluster after enabling EVC.

3 Ensure that the cluster contains hosts with CPUs from only one vendor, either Intel or AMD.

4 Edit the cluster settings and enable EVC.

   Select the CPU vendor and feature set appropriate for the hosts in the cluster.

5 If you powered off or migrated virtual machines out of the cluster, power on the virtual machines in the cluster, or migrate virtual machines into the cluster.

   Any virtual machines running with a larger feature set than the EVC mode you enabled for the cluster must be powered off before they can be moved back into the cluster.

Change the EVC Mode for a Cluster

If all the hosts in a cluster are compatible with the new mode, you can change the EVC mode of an existing EVC cluster. You can raise the EVC mode to expose more CPU features, or lower the EVC mode to hide CPU features and increase compatibility.

To raise the EVC mode from a CPU baseline with fewer features to one with more features, you do not need to turn off any running virtual machines in the cluster. Virtual machines that are running do not have access to the new features available in the new EVC mode until they are powered off and powered back on. A full power cycling is required. Rebooting the guest operating system or suspending and resuming the virtual machine is not sufficient.

To lower the EVC mode from a CPU baseline with more features to one with fewer features, you must first power off any virtual machines in the cluster that are running at a higher EVC mode than the one you intend to enable, and power them back on after the new mode has been enabled.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.
- If you intend to lower the EVC mode, power off any currently running virtual machines with a higher EVC mode than the one you intend to enable. See "Determine EVC Modes for Virtual Machines," on page 130.

Procedure

1 Display the cluster in the inventory.

2 Right-click the cluster and select **Edit Settings**.

3 In the left panel, select **VMware EVC**.

   The dialog box displays the current EVC settings.

4 To edit the EVC settings, click **Change EVC Mode**.

5 From the **VMware EVC Mode** drop-down menu, select the baseline CPU feature set you want to enable for the cluster.

   If the selected EVC Mode cannot be selected, the Compatibility pane displays the reason or reasons why, along with the relevant hosts for each reason.

6 Click **OK** to close the EVC Mode dialog box, and click **OK** to close the cluster settings dialog box.

Determine EVC Modes for Virtual Machines

The EVC mode of a virtual machine defines the CPU features that the virtual machine can access. The virtual machine's EVC mode is determined when it is powered on in an EVC-enabled cluster.

When a virtual machine is powered on, it determines the EVC mode of the cluster in which it is running. If the EVC mode of the cluster is subsequently raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not make use of any additional CPU features exposed by the cluster's new EVC mode until the virtual machine has been powered off and powered on again.

For example, consider a cluster containing hosts with Intel Xeon 45nm Core™ 2 processors that have been set to the Intel® "Merom" Generation (Xeon® Core™ 2) EVC mode. A virtual machine powered on in this cluster runs in the Intel "Merom" Generation (Xeon Core 2) EVC mode. If the cluster's EVC mode is raised to Intel "Penryn" Generation (Xeon 45nm Core 2), the virtual machine remains at the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use any of the features exposed by the higher cluster EVC mode, such as SSE4.1, you must power off the virtual machine and power it on again.

You can use the Virtual Machines tab of a cluster or a host to determine the EVC modes of the running virtual machines.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.

Procedure

1. Select the cluster or host in the inventory.
2. Click the **Virtual Machines** tab.
3. If the EVC Mode column is not displayed, right-click on the column titles and select **EVC Mode**.

   The EVC modes of all running or suspended virtual machines are displayed in the **EVC Mode** column. Powered off virtual machines and virtual machines that are not in EVC clusters show N/A as the EVC mode.

Prepare Clusters for AMD Processors Without 3DNow!

Newer generations of AMD processors do not include 3DNow! processor instructions. If hosts in a cluster have different generations of AMD processors, some with 3DNow! instruction sets and some without, you cannot successfully migrate virtual machines between the hosts. You must use an EVC mode or CPU compatibility mask to hide the instructions.

The vCenter Server **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode masks the 3DNow! instructions from virtual machines. You can apply this EVC mode to EVC clusters containing only AMD Opteron Generation 3 hosts to allow the clusters to maintain vMotion compatibility with AMD Opteron hosts that do not have 3DNow! instructions. Clusters containing AMD Opteron Generation 1 or AMD Opteron Generation 2 hosts cannot be made vMotion-compatible with hosts that do not have 3DNow! instructions.

Prerequisites

- You must be connected to a vCenter Server system with the vSphere Client.
- Ensure that the cluster contains only hosts with AMD Opteron Generation 3 or newer processors.

Procedure

◆ Enable the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode for your EVC cluster.

The steps to enable the EVC mode differ depending on whether you are creating a cluster or enabling the mode on an existing cluster, and on whether the existing cluster contains powered-on virtual machines.

Option	Description
Creating a new cluster	In the New Cluster wizard, enable EVC for AMD hosts and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster without powered-on virtual machines	In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster with powered-on virtual machines	The **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode cannot be enabled while there are powered-on virtual machines in the cluster. a Power-off any running virtual machines in the cluster, or migrate them out of the cluster using vMotion. Migrating the virtual machines out of the cluster with vMotion allows you to delay powering off the virtual machines until a more convenient time. b In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode. c If you migrated virtual machines out of the cluster, power them off and cold migrate them back into the cluster. d Power on the virtual machines.

You can now add hosts with AMD processors without 3DNow! instructions to the cluster and preserve vMotion compatibility between the new hosts and the existing hosts in the cluster.

View CPUID Details for an EVC Cluster

The feature set exposed by an EVC cluster corresponds to the feature set of a particular type of processor. Processor feature sets can be described by a set of feature flags that you can examine using the CPUID instruction.

You can view the CPUID feature flags currently exposed by the hosts in an EVC cluster using the Current CPUID Details dialog box.

Prerequisites

■ You must be connected to a vCenter Server system with the vSphere Client.

Procedure

1 Display the cluster in the inventory.

2 Right-click the cluster and select **Edit Settings**.

3 In the left panel, select **VMware EVC**.

4 To view the CPUID feature flags currently enforced by EVC, click **Current CPUID Details**.

The Current CPUID Details dialog box displays the CPUID feature flags that EVC is enforcing for the hosts in this cluster. For more information on CPUID feature flags, see *Intel Processor Identification and the CPUID Instruction* (available from Intel), or *CPUID Specification* (available from AMD).

Deploying OVF Templates 14

You can export virtual machines, virtual appliances, and vApps in Open Virtual Machine Format (OVF). You can then deploy the OVF template in the same environment or in a different environment.

This chapter includes the following topics:

- "Deploy an OVF Template in the vSphere Client," on page 133
- "Export an OVF Template," on page 134

Deploy an OVF Template in the vSphere Client

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

Procedure

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

The Deploy OVF Template wizard appears.

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

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

3 View the OVF Template Details page and click **Next**.

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

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

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

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

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

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

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

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

8 If the appliance that you are deploying has one ore more vService dependencies, select a binding service provider.

9 For each network specified in the OVF template, select a network by right-clicking the **Destination Network** column in your infrastructure to set up the network mapping and click **Next**.

10 On the **IP Allocation** page, configure how IP addresses are allocated for the virtual appliance and click **Next**.

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

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

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

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

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

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

Export an OVF Template

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

Required privilege: **vApp.Export**

Procedure

1 In the vSphere Client, select the virtual machine or vApp and select **File > Export > Export OVF Template**.

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

For example, type **`MyVm`**.

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

---

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

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

For example, **`OvfLib`**.

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

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

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

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

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

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

---

7 Click **OK**.

The download process is shown in the Export window.

Example: Folder Locations for OVF and OVA Files

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

- `C:\OvfLib\MyVm\MyVm.ovf`
- `C:\OvfLib\MyVm.mf`
- `C:\OvfLib\MyVm-disk1.vmdk`

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

- `C:\NewFolder\OvfLib\MyVm\MyVm.ovf`
- `C:\NewFolder\OvfLib\MyVm.mf`
- `C:\NewFolder\OvfLib\MyVm-disk1.vmdk`

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

Configuring Virtual Machines in the vSphere Client 15

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

This chapter includes the following topics:

- "Virtual Machine Limitations in the vSphere Client," on page 138
- "Virtual Machine Hardware Versions," on page 139
- "Locate the Hardware Version of a Virtual Machine in the vSphere Client," on page 140
- "Change the Virtual Machine Name in the vSphere Client," on page 141
- "View the Virtual Machine Configuration File Location in the vSphere Client," on page 141
- "Edit Configuration File Parameters in the vSphere Client," on page 141
- "Change the Configured Guest Operating System in the vSphere Client," on page 142
- "Configure Virtual Machines to Automatically Upgrade VMware Tools," on page 142
- "Virtual CPU Configuration," on page 143
- "Virtual Memory Configuration," on page 149
- "Network Virtual Machine Configuration," on page 153
- "Parallel and Serial Port Configuration," on page 154
- "Virtual Disk Configuration," on page 160
- "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 163
- "Other Virtual Machine Device Configuration," on page 167
- "Configuring vServices," on page 172
- "USB Configuration from an ESXi Host to a Virtual Machine," on page 173
- "USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client," on page 177
- "Manage Power Management Settings for a Virtual Machine," on page 180

- "Configure the Virtual Machine Power States," on page 180
- "Delay the Boot Sequence in the vSphere Client," on page 182
- "Enable Logging in the vSphere Client," on page 182
- "Disable Acceleration in the vSphere Client," on page 183
- "Configure Debugging and Statistics in the vSphere Client," on page 183

Virtual Machine Limitations in the vSphere Client

The virtual machine configuration tasks that you can perform when you connect directly to an ESXi host or vCenter Server system with the vSphere Client are limited.

The following virtual machine features are unavailable or read-only in the vSphere Client:

- Intel vGPU
- AMD vGPU
- 2TB HDD
- 128 vCPUs for virtual machines with hardware versions earlier than version 10
- 32 Serial Ports for virtual machines with hardware versions earlier than version 10
- 255 PVSCI devices
- SVGA for virtual machines with hardware versions 10 and 11
- VMCI firewall
- Smart card authentication
- SATA controller and hardware settings
- SR-IOV settings
- GPU 3D render and memory settings
- Tuning latency settings
- vSphere Flash Read Cache settings
- Nested hypervizor
- Fast checkpointing
- vCPU reference counters
- Ease and scheduled hardware upgrade
- Default compatibility level
- VMware Tools reporting and upgrade

Use the vSphere Web Client as the primary interface for managing the full range of virtual machine functions available in your vSphere 6.0 environment.

Virtual Machine Hardware Versions

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

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

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

Virtual machines with hardware versions earlier than version 11 can run on ESXi 6.0 hosts, but do not have all the capabilities available in hardware version 11. For example, you cannot use 128 virtual processors or 4080GB of memory in virtual machines with hardware versions earlier than version 11.

The vSphere Web Client and the vSphere Client allows you to upgrade virtual machines only to the latest hardware version. If virtual machines do not have to stay compatible with older ESX/ESXi hosts, you can upgrade them on ESXi 6.0 hosts. In this case, they are upgraded to version 11.

- To maintain virtual machine compatibility with ESX/ESXi 3.5 hosts, upgrade the virtual machine on an ESX/ESXi 3.5 host, which results in a virtual machine upgrade to version 4.
- To maintain virtual machine compatibility with ESX/ESXi 4.x hosts, upgrade the virtual machine on an ESX/ESXi 4.x host, which results in a virtual machine upgrade to version 7.
- To maintain virtual machine compatibility with ESXi 5.0 hosts, upgrade the virtual machine on an ESX/ESXi 5.0 host, which results in a virtual machine upgrade to version 8.
- To maintain virtual machine compatibility with ESXi 5.1 hosts, upgrade the virtual machine on an ESX/ESXi 5.1 host, which results in a virtual machine upgrade to version 9.
- To maintain virtual machine compatibility with ESXi 5.5 hosts, upgrade the virtual machine on an ESX/ESXi 5.5 host, which results in a virtual machine upgrade to version 10.

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

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

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

Table 15-1. ESXi Hosts and Compatible Virtual Machine Hardware Versions

	Version 11	Version 10	Version 9	Version 8	Version 7	Version 4	Compatible with vCenter Server Version
ESXi 6.0	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	vCenter Server 6.0
ESXi 5.5	Not supported	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	vCenter Server 5.5 and later
ESXi 5.1	Not supported	Not supported	Create, edit, run	Create, edit, run	Create, edit, run	Create, edit, run	vCenter Server 5.1 and later
ESXi 5.0	Not supported	Not supported	Not supported	Create, edit, run	Create, edit, run	Create, edit, run	vCenter Server 5.0 and later
ESX/ESXi 4.x	Not supported	Not supported	Not supported	Not supported	Create, edit, run	Create, edit, run	vCenter Server 4.x and later
ESX/ESXi 3.x	Not supported	Not supported	Not supported	Not supported	Not supported	Create, edit, run	vCenter Server 3.5 and later

Virtual machine hardware versions earlier than hardware version 4 are not supported on ESXi 6.0 hosts. To make full use of these virtual machines, upgrade the virtual hardware.

Note Virtual machine hardware versions 9, 10 and 11 features are limited to hardware version 8 and earlier when connected to the ESXi host or vCenter Server system using the vSphere Client.

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

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

Procedure

1 In the vSphere Client inventory, select the virtual machine.

2 Select a method for viewing the version information.

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

Change the Virtual Machine Name in the vSphere Client

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

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

Prerequisites

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

Procedure

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

View the Virtual Machine Configuration File Location in the vSphere Client

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

Prerequisites

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

Procedure

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

Edit Configuration File Parameters in the vSphere Client

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

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

The following conditions apply:

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced, click **General**.

3 Click **Configuration Parameters**.

4 (Optional) Change or add a parameter.

5 Click **OK** to exit the Configuration Parameters dialog box.

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

Change the Configured Guest Operating System in the vSphere Client

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

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

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and select **General Options**.

3 Select a guest operating system type and version.

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

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

Configure Virtual Machines to Automatically Upgrade VMware Tools

You can configure virtual machines to automatically update VMware Tools.

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

Prerequisites

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

Procedure

1 Right-click the virtual machine and click **Edit Settings**.

2 Click the **Options** tab and select **VMware Tools**.

3 Select **Check and upgrade Tools during power cycling** in the **Advanced** pane.

4 Click **OK** to save your changes and close the dialog box.

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

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters 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 CPU resource allocation strategy.

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

Change CPU Hot-Plug Settings in the vSphere Client

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

The following conditions apply:

- For best results, use virtual machines with hardware version 8 or later.
- Hot-adding multicore virtual CPUs is supported only with hardware version 8 or later.
- Not all guest operating systems support CPU hot add. You can disable these settings if the guest is not supported.
- To use the CPU hot-add feature with hardware version 7 virtual machines, set **Number of cores per socket** to 1.
- Adding CPU resources to a running virtual machine with CPU hot plug enabled disconnects and reconnects all USB passthrough devices connected to that virtual machine.

Prerequisites

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

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

Procedure

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

What to do next

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

Change the Number of Virtual CPUs

You can configure a virtual machine that runs on an ESXi host to have up to 128 virtual CPUs. You can change the number of virtual CPUs while the virtual machine is running or powered off.

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

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

Prerequisites

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

Procedure

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

   The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.
5. Click **OK** to save your changes.

Example: Adding Multicore CPU Resources to a Virtual Machine

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

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

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

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

Allocate CPU Resources in the vSphere Client

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

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

Limit Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz.

Reservation Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz.

Shares Each virtual machine is granted a number of CPU shares. The more shares a virtual machine has, the more often it gets a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

NOTE Virtual machine hardware versions 9, 10 and 11 features are read-only when connected to the ESXi host or vCenter Server system using the vSphere Client.

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab and select **CPU**.

3 Allocate the CPU capacity for this virtual machine.

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

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

Configuring Advanced CPU Scheduling Settings

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

Configure Hyperthreaded Core Sharing in the vSphere Client

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab and select **Advanced CPU**.

3 Select a mode from the **Hyperthreading Sharing Mode** drop-down menu.

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

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

Configure Processor Scheduling Affinity in the vSphere Client

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

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

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

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab and select **Advanced CPU**.

3 In the Scheduling Affinity panel, enter a comma-separated list of hyphenated processor ranges.

For example, "0,4-7" would indicate affinity with CPUs 0,4,5,6, and 7. Selecting all processors is identical to selecting no affinity. You must provide at least as many processor affinities as you have virtual CPUs.

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

Change CPU Identification Mask Settings in the vSphere Client

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

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced, select **CPUID Mask**.

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

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

4 (Optional) To edit mask values other than the NX bit or to set NX mask values to states other than “0” or “H”, click **Advanced**.

   a Select the relevant tab.

   b Click a row and edit the mask value.

      To view an explanation of a values symbol, click **Legend**.

   c Click **OK** to apply the changes and return to the Virtual Machine Properties dialog box.

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

Change CPU/MMU Virtualization Settings in the vSphere Client

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced, select **CPU/MMU Virtualization**.

3 Select an instruction set.

   - **Automatic**
   - **Use Software for instruction set and MMU**
   - **Use Intel VT-x/AMD-V for instruction set virtualization and software for MMU**
   - **Use Intel VT-x/AMD-V for instruction set virtualization and Intel EPT/AMD RVI for MMU virtualization**

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

Virtual Memory Configuration

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

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

Change the Memory Configuration in the vSphere Client

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

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

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

Table 15-2. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Version	Maximum Memory Size
ESXi 6.0	11	4080 GB
ESXi 5.5	10	1011 GB
ESXi 5.1	9	1011 GB
ESXi 5.0	8	1011 GB
ESX/ESXi 4.x	7	255 GB
ESX/ESXi 3.x	4	65532 MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a version 7 virtual machine running on ESXi 5.0 is restricted to 255 GB.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select **Memory**.

3 Adjust the amount of memory allocated to the virtual machine.

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

Allocate Memory Resources in the vSphere Client

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

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

Limit Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.

Reservation Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes.

Shares Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the more often it gets a time slice of a memory when no memory idle time is present. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the *vSphere Resource Management* documentation.

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

Note Virtual machine hardware versions 9, 10 and 11 features are read-only when connected to the ESXi host or vCenter Server system using the vSphere Client.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab and select **Memory**.

3 Allocated the memory capacity for this virtual machine.

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

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

Change Memory Hot-Add Settings in the vSphere Client

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced, select **Memory/CPU Hotplug**.

3 Enable or disable memory hot add.

- **Enable memory hot add for this virtual machine**.
- **Disable memory hot add for this virtual machine**.

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

Associate Memory Allocations with a NUMA Node in the vSphere Client

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

The following conditions apply to memory optimization with NUMA:

- The NUMA option is available on the Advanced Memory Resources page only if the host uses NUMA memory architecture.
- Affinity settings are meaningful only when used to modify the performance of a specific set of virtual machines on one host. This option is not available when the virtual machine resides on a DRS cluster. All affinity values are cleared when you move the virtual machine to a new host.
- You can specify nodes to use for future memory allocations only if you have also specified CPU affinity. If you make manual changes only to the memory affinity settings, automatic NUMA rebalancing does not work properly.

- Checking all the boxes is the same as applying no affinity.

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Select the **Resources** tab, and select **Memory**.

3 In the **NUMA Memory Affinity** panel, set the NUMA node affinity for the virtual machine.

- **No affinity**
- **Use memory from nodes**

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

Change the Swap File Location in the vSphere Client

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Option** tab and under Advanced, select **Swapfile Location**.

3 Select an option.

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

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

Network Virtual Machine Configuration

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

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

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

Prerequisites

Required Privileges:

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

Procedure

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

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

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

Option	Description
Standard settings	The virtual NIC connects to a standard or distributed port group. Select the port group for the virtual NIC to connect to from the **Network label** drop-down menu.
Advanced settings	The virtual NIC connects to a specific port on a vSphere distributed switch. This option appears only when a vSphere distributed switch is available. a Click **Switch to advanced settings**. b Select a vSphere distributed switch for the virtual NIC to use from the **VDS** drop-down menu. c Type the **Port ID** of the distributed port for virtual NIC to connect to.

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

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

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

Procedure

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

Parallel and Serial Port Configuration

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

Using Serial Ports with vSphere Virtual Machines

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

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

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

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

Server and Client Connections for Named Pipe and Network Serial Ports

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

Supported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, serial ports that are integrated into the motherboard are supported.

Unsupported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the following serial ports are not supported.

- Serial ports connected through USB are not supported for serial port passthrough. They might be supported by USB passthrough from an ESXi host to a virtual machine. See USB Configuration from an ESXi Host to a Virtual Machine.

In addition, you cannot use Migration with VMotion when you use a physical serial port for serial passthrough.

Adding a Firewall Rule Set for Serial Port Network Connections

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

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

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

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

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

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

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

Prerequisites

- Verify that the virtual machine is powered off.
- Familiarize yourself with the media types for the port to access, vSPC connections, and any conditions that might apply. See "Using Serial Ports with vSphere Virtual Machines," on page 154.
- To connect a serial port over a network, add a Firewall rule set. See Adding a Firewall Rule Set for Serial Port Network Connections.
- Required privilege: **Virtual Machine .Configuration.Add or Remove Device**

Procedure

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

Option	Description
Use physical serial port on the host	Click **Next** and select the port from the drop-down menu.
Output to file	Click **Next** and browse to the location of the file on the host to store the output of the virtual serial port.
Connect to named pipe	a Click **Next** and type a name for the pipe in the **Pipe Name** field. b Select the **Near end** and **Far end** of the pipe from the drop-down menus.
Connect via network	a Click **Next** and click**Server** or **Client** and type the Port URI. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. b If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator (vSPC)** and type the vSPC URI location.

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

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

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

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

```
telnet yourESXiServerIPAddress 12345
```

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

`telnet://yourLinuxBox:23`

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

Change the Serial Port Configuration in the vSphere Client

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

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

Prerequisites

- Check that you known the correct media types for the port to access, vSPC connections, and any conditions that might apply. See "Using Serial Ports with vSphere Virtual Machines," on page 154.
- To connect a serial port over a network, add a Firewall rule set. See Adding a Firewall Rule Set for Serial Port Network Connections.
- Required privilege: **Virtual machine.Configuration.Device connection**

Procedure

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

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

4. Select a connection type.

Option	Description
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port form the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.

Option	Description
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. 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	Select Use network to connect through a remote network. a Select the network backing. ■ Select **Server** to have the virtual machine monitor incoming connections from other hosts. ■ Select **Client** to have the virtual machine initiate a connection to another host. b Enter a **Port URI**. The URI is the remote end of the serial port to which the virtual machine's serial port 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) Select **Yield on poll**.

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

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

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

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

```
telnet yourESXiServerIPAddress 12345
```

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

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

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and click **Add**.

3 Select **Parallel Port** and click **Next**.

4 Select **Output to file** and click **Next**.

5 Browse to the location of the output file and Select or deselect the **Connect at power on** check box to connect or disconnect the device.

6 Click **Next**.

7 Review the information on the Ready to Complete page, and click **Finish**.

Change the Parallel Port Configuration in the vSphere Client

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

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

Virtual machines can be powered on during the configuration

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the parallel port to change.

3 Select **Output to file** and click **Browse** to navigate to the file location.

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

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

Configure Fibre Channel NPIV Settings in the vSphere Client

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

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

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

NPIV support is subject to the following limitations:

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

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

Prerequisites

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

Procedure

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

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

Virtual Disk Configuration

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

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

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

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

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

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

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

Change the Virtual Disk Configuration in the vSphere Client

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the hard disk to modify.

The name of the disk file and the disk type (thick or thin) appear in the upper-right pane.

3 Select a **Virtual Device Node** type from the drop-down menu.

This option is read-only when editing a virtual machine that is powered on.

4 To change the size of the disk, enter a new value in the **Provisioned Size** text box.

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

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

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

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

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and click **Add**.

3 Select **Hard Disk** and click **Next**.

4 Select the type of disk to use.

Option	Action
Create a new virtual disk	a Type the disk capacity. b Select a disk format. ■ **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. ■ **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. ■ **Thin Provision** creates a disk in thin format. Use this format to save storage space. c Select a location to store the disk. **Store with the virtual machine** or **Specify a datastore**. d If you selected **Specify a datastore**, browse for the datastore location, and click **Next**.
Use an Existing Virtual Disk	Browse for the disk file path and click **Next**.
Raw Device Mappings	Gives your virtual machine direct access to SAN. a Select the LUN to use for the raw disk, and click **Next**. b Select the datastore and click **Next**. c Select the compatibility mode. ■ **Physical** allows the guest operating system to access the hardware directly. ■ **Virtual** allows the virtual machine to use VMware snapshots and other advanced functions. d Click **Next**.

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

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

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

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

7 Click **Next**.

8 Review the information and click **Finish**.

9 Click **OK** to save your changes.

Use Disk Shares to Prioritize Virtual Machines in the vSphere Client

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

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

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab and select **Disk.**

3 In the Resource Allocation panel, select the virtual hard disk to change.

4 Click the **Shares** column and change the value to allocate a number of shares of its disk bandwidth to the virtual machine.

   - Low (500)
   - Normal (1000)
   - High (2000)
   - Custom

   When you select a shares symbolic value, the numeric value appears in the **Shares Value** column. You can select **Custom** to enter a user-defined shares value.

5 Click the **Limit - IOPS** column and enter the upper limit of storage resources to allocate to the virtual machine.

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

SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility

To access virtual disks, CD/DVD-ROM, and SCSI devices, a virtual machine uses storage controllers, which are added by default when you create the virtual machine. You can add additional controllers or change the controller type after virtual machine creation. You can make these changes while you are in the creation wizard. If you know about node behavior, controller limitations, and compatibility of different types of controllers before you change or add a controller, you can avoid potential boot problems.

How Storage Controller Technology Works

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. AHCI SATA controllers are also available.

When you create a virtual machine, the default controller is optimized for best performance. The controller type depends on the guest operating system, the device type, and in some cases, the virtual machine's compatibility. For example, when you create virtual machines with Apple Mac OS X guests and ESXi 5.5 and later compatibility, the default controller type for both the hard disk and the CD/DVD drive is SATA. When you create virtual machines with Windows Vista and later guests, a SCSI controller is the default for the hard disk and a SATA controller is the default for the CD/DVD drive.

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

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

If you add a SCSI controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:*z*), where 1 is SCSI controller 1 and *z* is a virtual device node from 0 to 15. For SCSI controllers, *z* cannot be 7. By default, the virtual SCSI controller is assigned to virtual device node (*z*:7), so that device node is unavailable for hard disks or other devices.

If you add a SATA controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:*z*), where 1 is SATA controller 1 and *z* is a virtual device node from 0 to 29. For SATA controllers, you can use device nodes 0 through 29, including 0:7.

Storage Controller Limitations

Storage controllers have the following requirements and limitations:

- LSI Logic SAS and VMware Paravirtual SCSI are available for virtual machines with ESXi 4.x and later compatibility.
- AHCI SATA is available only for virtual machines with ESXi 5.5 and later compatibility.
- BusLogic Parallel controllers do not support virtual machines with disks larger than 2TB.

Caution Changing the controller type after the guest operating system is installed will make the disk and any other devices connected to the adapter inaccessible. Before you change the controller type or add a new controller, make sure that the guest operating system installation media contains the necessary drivers. On Windows guest operating systems, the driver must be installed and configured as the boot driver.

Storage Controller Compatibility

Adding different types of storage controllers to virtual machines that use BIOS firmware can cause operating system boot problems. In the following cases, the virtual machine might fail to boot correctly and you might have to enter the BIOS setup and select the correct boot device:

- If the virtual machine boots from LSI Logic SAS or VMware Paravirtual SCSI, and you add a disk that uses BusLogic, LSI Logic, or AHCI SATA controllers.
- If the virtual machine boots from AHCI SATA, and you add BusLogic Parallel or LSI Logic controllers.

Adding additional disks to virtual machines that use EFI firmware does not cause boot problems.

Table 15-3. VMware Storage Controller Compatibility

	Added Controller					
Existing Controller	**BusLogic Parallel**	**LSI Logic**	**LSI Logic SAS**	**VMware Paravirtual SCSI**	**AHCI SATA**	**IDE**
BusLogic Parallel	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic SAS	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes
VMware Paravirtual SCSI	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes
AHCI SATA	Requires BIOS setup	Requires BIOS setup	Yes	Yes	Yes	Yes
IDE	Yes	Yes	Yes	Yes	Yes	N/A

Add SCSI Controllers

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

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

Prerequisites

Sufficient privileges to edit the virtual machine.

Procedure

1 Right-click on a virtual machine and select **Edit Settings**.

2 Select the Hardware tab.

3 Click **Add**.

4 Select **Hard Disk** and click **Next**.

5 Proceed through the wizard, selecting options that suit your needs.

6 In the Advanced Options page > Virtual Device Node section, select an unused SCSI Bus number.

For example, bus and device numbers 0:0 - 0:15 are used by the initial SCSI controller. The second SCSI controller uses bus and device numbers 1:0 - 1:15.

7 On the Ready to Complete page, click **Finish**.

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

Change the SCSI Bus Sharing Configuration in the vSphere Client

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select a SCSI Controller in the hardware list.

3 Select the type of sharing in the **SCSI Bus Sharing** list.

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

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

Change the SCSI Controller Type in the vSphere Client

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

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select a SCSI controller.

3 In the **SCSI Controller Type** pane, click **Change**.

4 Select a SCSI controller type and click **OK**.

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

About VMware Paravirtual SCSI Controllers

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

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

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

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

Add a Paravirtual SCSI Controller

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

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

Prerequisites

- Verify that the virtual machine has a guest operating system with VMware Tools installed.
- Verify that the virtual machine has hardware version 7 or later.
- Ensure that you are familiar with VMware Paravirtual SCSI limitations. See "About VMware Paravirtual SCSI Controllers," on page 166.
- 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 need to create a virtual machine with an LSI Logic controller, install VMware Tools, then change to paravirtual mode.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and click **Add**.

3 Select **SCSI Device** and click **Next**.

4 Select a SCSI device in the Connection panel.

5 Select an unused Virtual Device Node and click **Next**.

   For device node SCSI (0:2), 0 is the controller number and 2 is the number of the device that is attached to the controller. If you select a node on which devices already exist (for example, SCSI 0:3) you will add a SCSI device to the existing controller. To add a new controller, you must select an unused device node on an unused SCSI controller (for example 1:0).

6 Review your selections and click **Finish**.

   New SCSI Controller (adding) and **New SCSI Device (adding)** appear in the Hardware list.

7 Click **OK** to save your changes and exit the dialog box.

8 Reopen the Virtual Machine Properties Editor.

9 Select the new SCSI controller and click **Change Type**.

10 Select **VMware Paravirtual** and click **OK**.

11 Click **OK** to save your changes.

Other Virtual Machine Device Configuration

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

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

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Select the **Hardware** tab and click **Add**.

3 Select **CD/DVD Drive**, and click **Next**.

4 Select one option.

Option	Description
Use physical drive	a Select **Client** or **Host** as the location. b Select a **Pass through (recommended)** or **ATAPI emulation** connection type.
Use ISO Image	Enter the path and filename for the image file, or click **Browse** to navigate to the file.

5 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.

6 Click **Next**.

7 Select the virtual device node the drive uses in the virtual machine and click **Next**.

8 Review the information on the **Ready to Complete** window, and click **Finish** or click **Back** to change the settings.

9 Click **OK** to save your changes.

Change the CD/DVD Drive Configuration

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

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

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

Procedure

1 Select the virtual machine in the vSphere Client inventory.

2 Click the **CD/DVD Connections** icon on the virtual machine toolbar.

3 Select a drive or ISO image from the **CD/DVD drive** drop-down menu.

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

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

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the CD/DVD drive.

3 Select or deselect the **Connected** check box to connect or disconnect the device.

4 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.

5 Select **Host Device** under **Device Type** and select a device from the drop-down menu.

6 (Optional) In the drop-down menu under **Virtual Device Node**, select the node the drive uses in the virtual machine.

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the CD/DVD drive.

3 Select or deselect the **Connected** check box to connect or disconnect the device.

4 If you do not want the CD-ROM drive connected when the virtual machine starts, deselect **Connect at power on**.

5 Select **Datastore ISO File** under **Device Type** and click **Browse** to navigate to the file.

6 In the drop-down menu under **Virtual Device Node**, select the node the drive uses in the virtual machine.

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

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

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Select the **Hardware** tab and click **Add**.

3 Select **Floppy Drive**, and click **Next**.

4 Select the device type to use for this virtual device.

Option	Description
Use a physical floppy drive	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system running the vSphere Client. To connect the device, click the **Floppy Connections** button in the toolbar when you power on the virtual machine.
Use a floppy image	a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click **Browse** and select the floppy image.
Create a blank floppy image	a Select this option to create a floppy image on a datastore accessible to the host. b Click **Browse** and browse to the location for the floppy image. c Enter a name for the floppy image and click **OK**.

5 To have the floppy drive connected to the virtual machine when you power it on, select **Connect at power on**.

6 Click **Next**.

7 Review the information on the Ready to Complete page, and click **Finish**.

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

Change the Floppy Drive Configuration in the vSphere Client

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the Floppy drive.

3 Under Device Status, select **Connect at power on** to connect this virtual machine to the floppy drive when the virtual machine is powered on.

4 Select the device type to use for this virtual device.

Option	Description
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system running the vSphere Client. To connect the device, click the **Floppy Connections** button in the toolbar when you power on the virtual machine.
Use existing floppy image in datastore	a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click **Browse** and select the floppy image.
Create new floppy image in datastore	a Select this option to create a floppy image on a datastore accessible to the host. b Click **Browse** and browse to the location for the floppy image. c Enter a name for the floppy image and click **OK**.

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

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

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select **Add**.

3 Select **SCSI Device** and click **Next**.

4 Under **Connection**, use the drop-down menu to select a physical device.

5 Under **Virtual Device Node**, select the virtual device node where you want this device to appear in the virtual machine.

6 Review the information in the Ready to Complete page, and click **Finish**.

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

Change the SCSI Device Configuration in the vSphere Client

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select a SCSI device in the Hardware list.

3 Under **Connection**, select the physical device you want to use.

   Under Virtual device node, select the virtual device node where you want this device to appear in the virtual machine.

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

Add a PCI Device in the vSphere Client

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the Add Hardware wizard, select **PCI Device** and click **Next**.

4 Select the passthrough device to connect to the virtual machine from the drop-down list and click **Next**.

5 Click **Finish**.

Configure Video Cards in the vSphere Client

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

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

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

Prerequisites

Verify that the virtual machine is powered off.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select **Video card**.

3 Select the display settings type and configure the available settings.

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

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

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

5 Enter the video memory required for the displays.

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

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

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

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

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

Configuring vServices

A vService dependency allows a vApp or a virtual machine to request that a vService be available on a specified platform.

A vService specifies a particular service on which vApps and virtual machines can depend.

The vService configuration tab monitors and manages vService dependencies. This tab displays all the dependencies that a virtual machine or vApp has and each of their states. Each dependency shows the dependency name, description, requirement, bound status, and provider name.

Add a vService Dependency

You can add a vService dependency to a virtual machine or vApp. This dependency allows a virtual machine or vApp to request that a specific vService be available.

Procedure

1 Display the virtual machine or vApp in the inventory.

2 Power off the virtual machine or vApp.

3 Right-click the virtual machine or vApp and select **Edit Settings**.

4 Click the **vServices** tab.

5 Click **Add**.

6 In the Add Dependency wizard, select the provider for this dependency and click **Next.**

7 Enter the name and description for this dependency.

8 (Optional) If this dependency is required, select the check box and click **Next**.

   Required dependencies must be bound before powering on.

9 (Optional) If this dependency should be bound to the provider immediately, select the **Bind to provider immediately** check box, and click **Next** after the validation is complete.

   If you choose to bind this dependency now, the validation result displays. If the validation fails, you cannot complete adding the dependency. Deselect the check box to proceed.

10 Review the options and click **Finish** to create the dependency.

Edit a vService Dependency

You can edit a vService dependency name, description, and requirement.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine or vApp and select **Edit Settings**

2 From the **vServices** tab in the Edit Settings dialog box, right-click on the dependency and click **Edit**.

3 In the Dependency Properties dialog box, edit the dependency name and description.

4 Select or deselect the check box to change the required status of the dependency.

   The required check box is disabled if the virtual machine or vApp is running.

5 Select a provider for the dependency.

   When you select a provider, the description is entered containing the provider description. The validation box displays the results of the validation. If validation fails, the **OK** button is disabled until another provider or no provider is selected.

6 Click **OK**.

Remove a vService Dependency

You can remove a vService dependency from a virtual machine or vApp.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine or vApp and select **Edit Settings**

2 From the **vServices** tab in the Edit Settings dialog box, select the dependency and click **Remove**.

The dependency is removed from the list.

USB Configuration from an ESXi Host to a Virtual Machine

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

How USB Device Passthrough Technology Works

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

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

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

USB Arbitrator

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

USB Controller

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

USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist on the host. Eight virtual USB controllers are available to each virtual machine. A controller must be present before you can add USB devices to the virtual computer.

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

USB Devices

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine. The maximum number of USB devices supported on a single ESXi host for simultaneous connection to one or more virtual machines is also 20. For a list of supported USB devices, see the VMware knowledge base article at http://kb.vmware.com/kb/1021345. You can add USB 3.0 devices to Mac OSX guest operating system for VMware Fusion.

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

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

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

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

Table 15-4. USB Controller Support

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

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

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

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

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

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

1. In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
2. Click the **Hardware** tab and click **Add**.
3. Select **USB Controller** and click **Next**.
4. Select the Controller Type and click **Next**.
5. Click **Finish**.

   New USB Controller (adding) appears in the hardware list as **Present**.
6. Click **OK** to save your changes.

When you reopen the Properties Editor, the xHCI controller appears on the **Hardware** tab as USB xHCI controller. The EHCI+UHCI controller appears as **USB controller**.

What to do next

Add one or more USB devices to the virtual machine.

Remove a USB Controller from a Virtual Machine in the vSphere Client

You can remove a USB controller from a virtual machine if you do not want to connect to USB devices.

Prerequisites

- Verify that all USB devices are disconnected from the virtual machine.
- Required Privilege: **Virtual Machine.Configuration.Add or Remove Device**

Procedure

1. In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
2. Click the **Hardware** tab and select **USB controller**.
3. Click **Remove**.
4. Click **OK** to save your changes.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Add USB Devices from an ESXi Host to a Virtual Machine in the vSphere Client

You can add one or more USB passthrough devices from an ESXi host to a virtual machine if the physical device is connected to the host on which the virtual machine runs.

If a USB device is connected to another virtual machine, you cannot add it until that machine releases it.

NOTE If you have the Apple Frontpanel Controller device in your environment, you can safely add it to a virtual machine. However, this device has no documented function and no known use. ESXi hosts do not use it and do not provide Xserver functionality for USB passthrough

---

Prerequisites

- Verify that the virtual machine is using hardware version 7 or later.
- Verify that a USB controller is present. See "Add a USB Controller to a Virtual Machine in the vSphere Client," on page 174.
- To use vMotion to migrate a virtual machine with multiple USB devices, you must enable all attached USB devices for vMotion. You cannot migrate individual USB devices.
- When you add a CD/DVD-ROM drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.
- Verify that you know the virtual machine requirements for USB devices. See USB Configuration from an ESXi Host to a Virtual Machine.
- Required privileges: **Virtual Machine.Configuration.HostUSBDevice**

Procedure

1. In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
2. Click the **Hardware** tab and click **Add**.
3. Select **USB Device** and click **Next**.
4. (Optional) Select **Support vMotion while device is connected**.
5. If you do not plan to migrate a virtual machine with USB devices attached, deselect the **Support vMotion** option.

   This reduces migration complexity, which results in better performance and stability.
6. Select a device to add.

   You can add multiple USB devices, but only one device at a time.
7. Click **Finish**.

   New USB Device (adding) appears in the hardware list as **Present**.
8. Click **OK** to save your changes.

When you reopen the Properties editor, the USB device appears on the **Hardware** tab of the Properties Editor. The device type and ID appear in the right pane.

Remove a USB Device from a Virtual Machine

When you remove a USB device from a virtual machine, it reverts to the host and becomes available to other virtual machines that run on that host.

To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a "Remove Hardware" icon located in the System Tray. Linux operating systems use the **`umount`** command.

NOTE It might be necessary to use the **`sync`** command instead of or in addition to the **`umount`** command, for example after you issue a **`dd`** command on Linux or other UNIX operating systems.

Procedure

1 Unmount or eject the USB device from the guest operating system.

2 Right-click the virtual machine and select **Edit Settings**.

3 Click the **Hardware** tab and select the USB device.

4 Click **Remove** and click **OK** to save your changes and close the dialog box.

USB Configuration from a Client Computer to a Virtual Machine in the vSphere Client

You can add multiple USB devices to a virtual machine when the physical devices connect to a client computer on which the vSphere Client is running. The vSphere Client must be logged in to an instance of vCenter Server that manages the ESXi host or directly into the host where the virtual machines reside. USB passthrough technology supports adding multiple USB devices, such as security dongles, mass storage devices, and smartcard readers to virtual machines.

How USB Device Passthrough Technology Works

The USB controller is the USB hardware chip that provides USB function to the USB ports that it manages. USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist in the virtual machine. Two USB controllers are available for each virtual machine. The controllers support multiple USB 3.0, 2.0, and 1.1 devices. The controller must be present before you can add USB devices to the virtual machine.

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine.

You can add multiple devices to a virtual machine, but only one at a time. The virtual machine retains its connection to the device while in S1 standby. USB device connections are preserved when you migrate virtual machines to another host in the datacenter.

A USB device is available to only one powered-on virtual machine at a time. When a virtual machine connects to a device, that device is no longer available to other virtual machines or to the client computer. When you disconnect the device from the virtual machine or shut the virtual machine down, the device returns to the client computer and becomes available to other virtual machines that the client computer manages.

For example, when you connect a USB mass storage device to a virtual machine, it is removed from the client computer and does not appear as a drive with a removable device. When you disconnect the device from the virtual machine, it reconnects to the client computer's operating system and is listed as a removable device.

USB 3.0 Device Limitations

USB 3.0 devices have the following requirements and limitations:

- The virtual machine that you connect the USB 3.0 device to must be configured with an xHCI controller and have a Linux guest operating system with a 2.6.35 or later kernel.
- You can connect only one USB 3.0 device operating at superspeed to a virtual machine at a time.
- USB 3.0 devices are available only for passthrough from a client computer to a virtual machine. They are not available for passthrough from an ESXi host to a virtual machine.

Avoiding Data Loss

Before you connect a device to a virtual machine, make sure the device is not in use on the client computer.

If the vSphere Client disconnects from the vCenter Server or host, or if you restart or shut down the client computer, the device connection breaks. It is best to have a dedicated client computer for USB device use or to reserve USB devices connected to a client computer for short-term use, such as updating software or adding patches to virtual machines. To maintain USB device connections to a virtual machine for an extended time, use USB passthrough from an ESXi host to the virtual machine.

Connect USB Devices to a Client Computer

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

The number of ports on each client computer depends on the physical setup of the client. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

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

Prerequisites

Verify that you know the requirements for configuring USB devices from a remote computer to a virtual machine.

Procedure

- To add a USB device to a client computer, connect the device to an available port or hub.

The USB device appears in the virtual machine toolbar menu.

What to do next

You can now add the USB device to the virtual machine.

Add USB Devices From a Client Computer to a Virtual Machine in the vSphere Client

You can add one or more USB passthrough devices from a client computer to a virtual machine in the vSphere Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machines reside.

The devices maintain their virtual machine connections in S1 standby, if the vSphere Client is running and connected. After you add the USB device to the virtual machine, an information message appears on the client computer stating that the device is disconnected. The device remains disconnected from the client computer until the virtual machine releases it.

FT is not supported with USB passthrough from a client computer to a virtual machine.

Prerequisites

- Verify that a USB controller is installed.
- Verify that the vSphere Client is connected to the ESXi host on which the virtual machines are running.
- Required Privilege: **Virtual Machine.Interaction.Add or Remove Device**

Procedure

1. Select the virtual machine in the vSphere Client inventory.
2. Click the USB icon on the virtual machine toolbar.
3. Select an available device from the **Connect to USB Devices** drop-down menu.

   The status of the device appears as Connecting.

The device appears in the **USB Connections** drop-down menu and is ready to use. The device remains connected until you power off the virtual machine or disconnect the vSphere Client from the ESXi host.

Remove USB Devices That Are Connected Through a Client Computer in the vSphere Client

You can remove USB devices from a virtual machine if the devices are no longer needed. When you disconnect a USB device from a virtual machine, the device is released from the virtual machine and is given back to the client computer, which starts using it.

Prerequisites

To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a "Remove Hardware" icon located in the System Tray. Linux operating systems use the **`umount`** command.

NOTE You might need to use the `sync` command instead of or in addition to the `umount` command, for example after you run a `dd` command on Linux or other UNIX operating systems.

Procedure

1. Unmount or eject the USB device from the guest operating system.
2. Select the virtual machine in the vSphere Client inventory.
3. Click **USB Connections** on the virtual machine toolbar.

4 Select the device to remove from the drop-down menu.

   For example, select **USB Device 1 > Disconnect from** *device name*.

   The menu shows the device status as Disconnecting.

The device reconnects to the client computer and is available to add to another virtual machine. In some cases, Windows Explorer detects the device and opens a dialog box on the client computer. You can close this dialog box.

Manage Power Management Settings for a Virtual Machine

You can set the power options so that a virtual machine is suspended or remains powered on when the guest operating system is placed on standby.

Power Management options are not available on every guest operating system. **Wake on LAN** supports only Windows guest operating systems and is not available on Vlance NICs, or when a Flexible NIC is operating in Vlance mode (that is, the current VMware Tools are not installed on the guest operating system).

Wake on LAN can resume virtual machines that are in an S1 sleep state only. It cannot resume suspended, hibernated, or powered off virtual machines.

The following NICs support **Wake on LAN**:

- Flexible (VMware Tools required).
- vmxnet
- Enhanced vmxnet
- vmxnet 3

Prerequisites

You must power off the virtual machine.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and expand **Power Management**.

3 Select a power option.

   - **Suspend the virtual machine**
   - **Put the guest OS into standby mode and leave the virtual machine powered on**

4 (Optional) Select **Wake on LAN for virtual machine traffic on** and select the virtual NICs to trigger this action.

   Unsupported NICs might be listed, but are unavailable to connect.

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

Configure the Virtual Machine Power States

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

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

Table 15-5 lists available power buttons and describes their behavior.

Table 15-5. Virtual Machine Power Button Settings

Power Button	Description
	Shuts down the guest operating system or powers off the virtual machine. A power off operation displays a confirmation dialog box indicating that the guest operating system might not shut down properly. Use this power off option only when necessary.
	Suspends the virtual machine without running a script when VMware Tools is not installed. When VMware Tools is installed and available, a suspend action runs a script, and suspends the virtual machine.
	Powers on a virtual machine when a virtual machine is stopped, or resumes the virtual machine and runs a script when it is suspended and VMware Tools is installed and available. Resumes the virtual machine and does not run a script when VMware Tools is not installed.
	Resets the virtual machine when VMware Tools is not installed. Restarts the guest operating system when VMware Tools is installed and available. A reset operation displays a confirmation dialog box indicating that the guest operating system is not shut down properly.

Prerequisites

- Verify that you have access to at least one virtual machine in the inventory.
- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, you must install VMWare Tools in the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and select **VMware Tools**.

3 In the right panel, select the **Power Controls** for the virtual machine.

4 Select an option for the **Power Off** button.

Option	Description
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. This type of powering off is known as a "soft" power operation. Soft power operations are possible only if the tools are installed in the guest operating system.
Power Off	Immediately stops the virtual machine. This type of powering off is known as a "hard" power operation.
System Default	Follows system settings. The current value of the system settings is shown in parentheses.

5 Select an option for the **Suspend** button.

Option	Description
Suspend	Pauses all virtual machine activity.
System Default	Follows system settings. The current value of the system setting is shown in parentheses.

6 Select an option for the **Reset** button.

Option	Description
Restart Guest	Uses VMware Tools to initiate an orderly reboot. (This type of reset is known as a "soft" power operation. Soft power operations are possible only if the tools are installed in the guest operating system.)
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. (This type of reset is known as a "hard" power operation.)
System Default	Follows system settings; the current value of the system setting is shown in parentheses.

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

What to do next

Configure VMware Tools scripts to run before or after power operations.

Delay the Boot Sequence in the vSphere Client

The time between when you power on the virtual machine and when it exits the BIOS or EFI and launches the guest operating system software can be short. You can change the boot delay or force the virtual machine to enter the BIOS or EFI setup screen after power on.

Delaying the boot operation is useful for changing BIOS or EFI settings such as the boot order. For example, you can change the BIOS or EFI settings to force a virtual machine to boot from a CD-ROM.

Prerequisites

Required Privilege: **Virtual machine.Configuration.Settings**

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced select **Boot Options**.

3 In the **Power on Boot Delay** panel, select the time in milliseconds to delay the boot operation.

4 (Optional) Select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.

5 (Optional) Select whether to try to reboot after a boot failure.

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

Enable Logging in the vSphere Client

You can enable logging to collect log files to help troubleshoot issues with your virtual machine.

Required privilege: **Virtual machine.Configuration.Settings**

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced select **General**.

3 In the **Settings** pane, select **Enable logging**.

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

Disable Acceleration in the vSphere Client

You can temporarily disable acceleration to allow a virtual machine to successfully run or install software.

In rare instances, you might find that when you install or run software in a virtual machine, the virtual machine appears to stop responding. Generally, the problem occurs early in the program's execution. Often, you can get past the problem by temporarily disabling acceleration in the virtual machine.

Disabling acceleration slows down virtual machine performance. You must enable acceleration after the program stops encountering problems to run the program with acceleration.

You can enable and disable acceleration when the virtual machine is running.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Options** tab and under Advanced select **General**.

3 In the **Settings** pane, select **Disable acceleration**.

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

Configure Debugging and Statistics in the vSphere Client

You can run a virtual machine so that it collects debugging information and statistics that are helpful to VMware technical support in resolving issues.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**

2 Click the **Options** tab and under Advanced select **General**.

3 To enable debugging mode, select an option from the **Debugging and Statistics** pane.

- **Run normally**
- **Record Debugging Information**
- **Record Statistics**
- **Record Statistics and Debugging**

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

Managing Virtual Machines 16

When you connect directly to an ESXi host or vCenter Server system using the vSphere Client, you can open a console to any of the host's virtual machines, add and remove virtual machines in the host's inventory, and manage virtual machine snapshots.

This chapter includes the following topics:

- "Edit Virtual Machine Startup and Shutdown Settings," on page 185
- "Open a Console to a Virtual Machine," on page 186
- "Adding and Removing Virtual Machines," on page 186
- "Using Snapshots To Manage Virtual Machines," on page 187

Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host. You can also set the default timing and startup order for selected virtual machines. This ability allows the operating system to save data when the host enters maintenance mode or is being powered off for another reason.

The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located and click the **Configuration** tab.
2. Under Software, click **Virtual Machine Startup/Shutdown** and click **Properties**.

   The Virtual Machine Startup and Shutdown dialog box opens.
3. Select **Allow virtual machines to start and stop automatically with the system**.
4. (Optional) Configure the startup and shutdown behavior.

Option	Action
Default Startup Delay	Select the amount of time to delay starting the operating system. This delay allows time for VMware Tools or the booting system to run scripts.
Continue immediately if the VMware Tools starts	Select to start the operating system immediately after VMware Tools starts.

Option	Action
Default Shutdown Delay	Select the amount of time to delay shutdown for each virtual machine. The shutdown delay applies only if the virtual machine does not shut down before the delay period elapses. If the virtual machine shuts down before the delay time is reached, the next virtual machine starts shutting down.
Shutdown Action	Select a shutdown option from the drop-down menu. ■ Power Off ■ Suspend ■ Guest Shutdown
Move Up and Move Down	Select a virtual machine in the Manual Startup category and use the **Move Up** button to move it up to Automatic Startup or Any Oder. When virtual machines are in the Automatic Startup category, you can use **Move Up** and **Move Down** to order them so that they start in a preferred sequence. During shutdown, the virtual machines are stopped in the opposite order.
Edit	Click **Edit** to configure user-specified autostartup and shutdown behavior for virtual machines in the Automatic Startup or Any Order category.

5 Click **OK** to close the dialog box and save your settings.

Open a Console to a Virtual Machine

With the vSphere Client, you can access a virtual machine's desktop by launching a console to the virtual machine. From the console, you can perform activities within the virtual machine such as configure operating system settings, run applications, monitor performance, and so on.

Procedure

1 In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

2 In the **Commands** section, select **Open Console**.

3 Click anywhere inside the console window to enable your mouse, keyboard, and other input devices to work in the console.

Adding and Removing Virtual Machines

You add virtual machines to the vCenter Server inventory through their managed hosts. You can remove virtual machines from vCenter Server, from their managed host's storage, or from both.

Remove Virtual Machines from a Host

Removing a virtual machine from the inventory unregisters it from the host, but does not delete it from the datastore. Virtual machine files remain at the same storage location and the virtual machine can be re-registered by using the datastore browser.

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Remove from Inventory**.

2 To confirm that you want to remove the virtual machine from the inventory, click **Yes**.

The host removes references to the virtual machine and no longer tracks its condition.

Remove Virtual Machines from the Datastore

You use the **Delete from Disk** option to remove a virtual machine from a host and delete all virtual machine files, including the configuration file and virtual disk files, from the datastore.

Prerequisites

Power off the virtual machine.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Delete from Disk**.

2 Click **Yes** in the confirmation dialog box.

The host deletes the virtual machine from its datastore. Disks that are shared with other virtual machines are not deleted.

Return a Virtual Machine or Template to a Host

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

Procedure

1 In the vSphere Client, navigate to **Home > Inventory > Datastores and Datastore Clusters**.

2 Right-click the datastore and select **Browse Datastore**.

3 Navigate to the virtual machine or template folder to add to the inventory.

4 Right-click the virtual machine or template `.vmx` file and select **Add to Inventory**.

5 Complete the Add to Inventory wizard to add the virtual machine or template.

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking snapshots for all members of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before diverging a virtual machine in the snapshot tree.

The Snapshot Manager in the vSphere Web Client and the vSphere Client provide several operations for creating and managing virtual machine snapshots and snapshot trees. These operations let you create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create extensive snapshot trees that you can use to save the virtual machine state at any specific time and restore the virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes disks that were added or changed after you took the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The Snapshot Manager presents the snapshot hierarchy as a tree with one or more branches. The relationship between snapshots is like that of a parent to a child. In the linear process, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshots. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or restore any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you restore a snapshot and take another snapshot, a branch, or child snapshot, is created.

Parent Snapshots

The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base .vmdk file. The parent snapshot is always the snapshot that appears immediately above the You are here icon in the Snapshot Manager. If you revert or restore a snapshot, that snapshot becomes the parent of the You are here current state.

Note The parent snapshot is not always the snapshot that you took most recently.

Child Snapshots

A snapshot that is taken of the same virtual machine after the parent snapshot. Each child constitutes delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

Important Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk using `vmkfstools`.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta `.vmdk` disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base `.vmdk` file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Taking Snapshots of a Virtual Machine

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

Memory Snapshots

The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.

Quiesced Snapshots

When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

If the virtual machine is powered off or VMware Tools is not available, the `Quiesce` parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

Important Do not use snapshots as your only backup solution or as a long-term backup solution.

Change Disk Mode to Exclude Virtual Disks from Snapshots in the vSphere Client

You can set a virtual disk to independent mode to exclude the disk from any snapshots taken of its virtual machine.

Prerequisites

Power off the virtual machine and delete any existing snapshots before you change the disk mode. Deleting a snapshot involves committing the existing data on the snapshot disk to the parent disk.

Required privileges:

- **Virtual machine.Snapshot management.Remove Snapshot**
- **Virtual machine.Configuration.Modify device settings**

Procedure

1 In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and select the hard disk to exclude.

3 Under **Mode**, select **Independent**.

Snapshots do not affect the state of an independent disk.

Note Any disk, regardless of its type, that is created after you take a snapshot does not appear if you revert to that snapshot.

4 Select an independent disk mode option.

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

5 Click **OK**.

Take a Snapshot in the vSphere Client

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. If you are suspending a virtual machine, wait until the suspend operation finishes before you take a snapshot.

When you create a memory snapshot, the snapshot captures the state of the virtual machine's memory and the virtual machine power settings. When you capture the virtual machine's memory state, the snapshot operation takes longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stored on the disk during a restore operation.

Note You cannot revert to a snapshot with dynamic disks, so quiesced snapshots are not used when you restore dynamic disks. Snapshot technology has no visibility into Dynamic Disks. Dynamic Disks are commonly known as Microsoft specific file systems.

Prerequisites

- If you are taking a memory snapshot of a virtual machine that has multiple disks in different disk modes, verify that the virtual machine is powered off. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- To capture the memory state of the virtual machine, verify that the virtual machine is powered on.
- To quiesce the virtual machine files, verify that the virtual machine is powered on and that VMware Tools is installed.
- Required privilege: **Virtual machine.Snapshot management. Create snapshot** on the virtual machine.

Procedure

1. In the vSphere Client inventory, right-click the virtual machine and select **Snapshot > Take Snapshot**.
2. Type a name for the snapshot.
3. Type a description for the snapshot.

   Adding a date and time or a description, for example, "Snapshot before applying XYZ patch," can help you determine which snapshot to restore or delete.
4. (Optional) When the virtual machine is powered on, select the **Snapshot the virtual machine's memory** check box to capture the memory of the virtual machine.
5. (Optional) When the virtual machine is powered on, select the **Quiesce guest file system (Needs VMware Tools installed)** check box to pause running processes on the guest operating system so that file system contents are in a known consistent state when you take the snapshot.
6. Click **OK**.

After you take the snapshot, you can view its status in the **Recent Tasks** field at the bottom of the vSphere Client.

Restoring Snapshots

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can restore a snapshot.

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot. If you want the virtual machine to be suspended, powered on, or powered off when you start it, make sure that it is in the correct state when you take the snapshot.

You can restore snapshots in the following ways:

Revert to 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 16-1. Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Note vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

Revert to a Snapshot in the vSphere Client

You can restore the parent snapshot of the current state of the virtual machine.

When you revert to a snapshot, disks that you added or changed after the snapshot was taken are reverted to the snapshot point. For example, when you take a snapshot of a virtual machine, add a disk, and revert the snapshot, the added disk is removed.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Revert to snapshot** on the virtual machine.

Procedure

- Right-click a virtual machine in the vSphere Client inventory and select **Revert to Current Snapshot**.

The virtual machine power and data states are returned to the states they were in at the time you took the parent snapshot. If the parent snapshot is a memory snapshot, the virtual machine is restored to an on power state.

Go To a Snapshot in the vSphere Client

You can go to any snapshot in the snapshot tree to restore the virtual machine to the state of that snapshot.

Note Virtual machines running certain kinds of workloads might take several minutes to resume responsiveness after reverting from a snapshot.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Revert to snapshot** on the virtual machine

Procedure

1. Right-click a virtual machine in the vSphere Client inventory and select **Snapshot Manager**.
2. In the Snapshot Manager, click a snapshot to select it.
3. Click **Go to** to restore the virtual machine to the snapshot.

4 Click **Yes** in the confirmation dialog box.

Subsequent child snapshots from this point create a new branch of the snapshot tree. The delta disks for snapshots that you took after you restored the current snapshot are not removed and you can restore those snapshots at any time.

Deleting Snapshots

Deleting a snapshot removes the snapshot from the Snapshot Manager. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk.

Deleting a snapshot leaves the current state of the virtual machine or any other snapshot untouched. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes to the parent disk all data from the delta disk that contains the information about the deleted snapshot. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

Deleting snapshots involves large amounts of disk reads and writes, which can reduce virtual machine performance until consolidation is complete. Consolidating snapshots removes redundant disks, which improves virtual machine performance and saves storage space. The time it takes to delete snapshots and consolidate the snapshot files depends on the volume of data that the guest operating system wrote to the virtual disks after you took the last snapshot. The required time is proportional to the amount of data the virtual machine is writing during consolidation if the virtual machine is powered on.

If disk consolidation fails when you delete a snapshot or delete all snapshots and you notice a degradation in virtual machine performance, you can view a list of virtual machines to determine if any files require consolidation, and if so, run a separate consolidation operation. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see "Consolidate Snapshots in the vSphere Client," on page 194

Delete

Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes between the snapshot and the previous delta disk state to the parent snapshot.

You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.

Delete All

Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes changes between snapshots and previous delta disk states to the base parent disk and merges them with the base virtual machine disk.

To prevent snapshot files from merging with the parent snapshot, for example in cases of failed updates or installations, first use the **Go to** command to restore to a previous snapshot. This action invalidates the snapshot delta disks and deletes the memory file. You can then use the **Delete** option to remove the snapshot and any associated files.

Delete a Snapshot in the vSphere Client

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

Use care when you delete snapshots. You cannot restore a deleted snapshot. For example, you might want to install several browsers, a, b, and c, and capture the virtual machine state after you install each browser. The first, or base snapshot, captures the virtual machine with browser a and the second snapshot captures browser b. If you restore the base snapshot that includes browser a and take a third snapshot to capture browser c and delete the snapshot that contains browser b, you cannot return to the virtual machine state that includes browser b.

Prerequisites

- Ensure that you are familiar with the Delete and Delete all actions and how they might affect virtual machine performance. See "Deleting Snapshots," on page 193.
- Required Privilege: **Virtual machine.Snapshot management.Remove Snapshot** on the virtual machine.

Procedure

1 Select **Inventory > Virtual Machine > Snapshot > Snapshot Manager**.

2 In the Snapshot Manager, click a snapshot to select it.

3 Select a delete option.

Option	Description
Delete	Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine.
Delete All	Consolidates all of the immediate snapshots before the You are here current state to the base parent disk and removes all existing snapshots from the Snapshot Manager and virtual machine.

4 Click **Yes**.

Consolidate Snapshots in the vSphere Client

The snapshot Consolidation command searches for hierarchies or delta disks to combine without violating data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compact after a **Delete** or **Delete all** operation or if the disk did not consolidate. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

The Needs Consolidation column in the vSphere Client shows the virtual machines that need to be consolidated and the virtual machine's **Summary** tab shows a Configuration Issues consolidation message if the virtual machine needs to be consolidated. If you see errors for failed conditions, such as running out of disk space, correct them and run the consolidation task.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Remove Snapshot**

Procedure

1 Display the Need Consolidation column in the vSphere Client.

   a Select a vCenter Server, host, or cluster and click the **Virtual Machines** tab.

   b Right-click the menu bar for any virtual machine column and select **Needs Consolidation** from the menu.

   The Needs Consolidation column appears. A Yes status indicates that the snapshot files for the virtual machine should be consolidated and that the virtual machine's **Tasks and Events** tab shows a configuration problem. A No status indicates that the files are OK.

2 To consolidate the files, right-click the virtual machine and select **Snapshot > Consolidate**.

3 Check the Need Consolidation column to verify that the task succeeded.

   If the task succeeded, the Configuration Issues message should be cleared and the Needs Consolidation value should be No.

Managing Multi-Tiered Applications with vSphere vApp in the vSphere Client

17

You can use VMware vSphere as a platform for running applications, in addition to using it as a platform for running virtual machines. The applications can be packaged to run directly on top of VMware vSphere. The format of how the applications are packaged and managed is called vSphere vApp.

A vApp is a container, like a resource pool and can contain one or more virtual machines. A vApp also shares some functionality with virtual machines. A vApp can power on and power off, and can also be cloned.

In the vSphere Client, a vApp is represented in both the Host and Clusters view and the VM and Template view. Each view has a specific summary page with the current status of the service and relevant summary information, as well as operations on the service.

The distribution format for vApp is OVF.

Note The vApp metadata resides in the vCenter Server's database, so a vApp can be distributed across multiple ESXi hosts. This information can be lost if the vCenter Server database is cleared or if a standalone ESXi host that contains a vApp is removed from vCenter Server. You should back up vApps to an OVF package to avoid losing any metadata.

vApp metadata for virtual machines within vApps do not follow the snapshots semantics for virtual machine configuration. So, 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 prior snapshots.

You can use VMware Studio to automate the creation of ready-to-deploy vApps with pre-populated application software and operating systems. VMware Studio adds a network agent to the guest so that vApps bootstrap with minimal effort. Configuration parameters specified for vApps appear as OVF properties in the vCenter Server deployment wizard. For information about VMware Studio and for download, see the VMware Studio developer page on the VMware web site.

This chapter includes the following topics:

- "Create a vApp," on page 196
- "Power On a vApp in the vSphere Client," on page 197
- "Clone a vApp," on page 198
- "Power Off a vApp in the vSphere Client," on page 198
- "Suspend a vApp in the vSphere Client," on page 198
- "Resume a vApp in the vSphere Client," on page 199
- "Populate the vApp," on page 199
- "Edit vApp Settings in the vSphere Client," on page 200

- "Configuring IP Pools," on page 204
- "Edit vApp Annotation in the vSphere Client," on page 206

Create a vApp

A vApp allows you to perform resource management and certain other management activities such as power operations for multiple virtual machines at the same time. You can think of the vApp as the container for the virtual machines, and you can perform the operations on the container.

When you create a vApp, you can add it to a folder, standalone host, resource pool, cluster enabled for DRS, or another vApp.

Prerequisites

Verify that one of those objects is available in your datacenter.

- A standalone host that is running ESX 4.0 or greater.
- A cluster that is enabled for DRS.

Procedure

1. Navigate to an object that supports vApp creation and select the New vApp icon ( ).
2. In the **vApp Name** text box, type a name for the vApp.
3. Select the vApp Inventory Location and click **Next**.
   - If you start the action from a folder or vApp, you are prompted for a host, cluster, or resource pool.
   - If you start the action from a resource pool, host, or cluster, you are prompted for a folder or data center.

4 In the Resource Allocation page, allocate CPU and memory resources to this vApp.

a Allocate CPU resources for this vApp.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps 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 vApp a specific number of shares, which express a proportinal weight.
Reservation	Guaranteed CPU allocation for this vApp.
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select **Unlimited** to specify no upper limit.

b Allocate memory resources for this vApp.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps 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 vApp a specific number of shares, which express a proportinal weight.
Reservation	Guaranteed memory allocation for this vApp.
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select **Unlimited** to specify no upper limit.

5 Click **Next**.

6 Review the vApp settings and click **Finish**.

Power On a vApp in the vSphere Client

Each virtual machine within the vApp is powered on according to the startup order configuration.

When powering on a vApp within a DRS cluster in manual mode, no DRS recommendations are generated for virtual machine placements. The power-on operation performs as if DRS is run in a semiautomatic or automatic mode for the initial placements of the virtual machines. This does not affect vMotion recommendations. Recommendations for individual powering on and powering off of virtual machines are also generated for vApps that are running.

Procedure

◆ In the Summary page for the service, click **Power On**.

If a delay is set in the startup settings, the vApp waits for the set length of time before powering up that virtual machine.

In the **Summary** tab, the status indicates when the vApp has started and is available. Links to the product and vendor Web sites are also found under the General section.

Clone a vApp

Cloning a vApp is similar to cloning a virtual machine.

Prerequisites

To clone a vApp, the vSphere Client must be connected to the vCenter Server system.

A host must be selected in the inventory that is running ESX 4.0 or greater, or a cluster enabled with DRS.

Procedure

1 Select the vApp in the inventory.

2 Select **Inventory > vApp > Clone**.

Complete each page in Clone vApp the wizard.

3 Select the vApp destination and click **Next**.

4 Specify a Host and click **Next**.

NOTE This step is available only if you select a cluster that is in DRS manual mode.

5 Enter a name for the vApp clone and select the **vApp Inventory Location**, then click **Next**.

6 Select a datastore and click **Next**.

7 Select a disk format to store the virtual machines virtual disks and click **Next**.

- **Same format as source**
- **Thin provisioned format**
- **Thick format**

8 Review the new vApp settings and click **Finish**.

Power Off a vApp in the vSphere Client

Each virtual machine within the vApp is powered off in reverse order to how they are configured for startup.

Procedure

◆ In the Summary page for the service, click **Power Off**.

If a delay is set in the shutdown settings, the vApp waits for the set length of time before powering down that virtual machine.

Suspend a vApp in the vSphere Client

A suspended vApp pauses all its running virtual machines until you resume the vApp.

The virtual machines within a vApp are suspended based on their stop order. All virtual machines are suspended regardless of stop action.

Procedure

1 From the vSphere Client select the vApp you want to place in suspended state.

2 Right-click the vApp and select **Suspend**.

Resume a vApp in the vSphere Client

You can continue the activity of the virtual machines within a vApp that is in a suspended state.

The suspended virtual machines within the vApp are resumed in reverse order to the order in which they were suspended.

Procedure

1 From the vSphere Client, select the vApp.

2 Right-click the vApp and select **Power On**.

Populate the vApp

Virtual machines and other vApps can be added to and removed from a vApp.

After you create a vApp, you can populate it with virtual machines or other vApps.

Create an Object Inside the vApp in the vSphere Client

Within a vApp, you can create a new virtual machine, resource pool, or another vApp.

Procedure

1 In the inventory, select the vApp in which you want to create the object machine.

2 Select the menu option to create a specific object.

Menu Option	Description
Inventory > vApp > New Virtual Machine	Creates a new virtual machine inside the vApp. Complete the Create New Virtual Machine wizard. See Chapter 10, "Creating a Virtual Machine in the vSphere Client," on page 85 for instructions on creating a new virtual machine.
Inventory > vApp > New Resource Pool	Adds a resource pool inside the vApp. Complete the Create Resource Pool window.
Inventory > vApp > New vApp	Creates a new vApp inside the currently selected vApp. Complete the New vApp wizard. See "Create a vApp," on page 196 for instructions on creating a new vApp.

The new object appears as part of the vApp in the inventory.

Add an Object to a vApp in the vSphere Client

You can add an object, such as a virtual machine or another vApp, to an existing vApp.

An existing virtual machine or another vApp that is not already contained inside the vApp can be moved into the currently selected vApp.

Procedure

1 Display the object in the inventory.

2 Click and drag the object to the target object.

- If the move is permitted, a box appears around the target-object, indicating it is selected.
- If the move is not permitted, a naught sign (zero with a slash) appears, and the object is not moved.

3 Release the mouse button.

Either the object moves to the new location or an error message indicates what needs to be done to permit the move.

Edit vApp Settings in the vSphere Client

You can edit and configure several vApp settings, including startup order, resources, and custom properties.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click the **Options** tab to edit or view vApp properties.

NOTE The deployer typically edits the IP allocation policy and properties. The vApp author typically edits the other, more advanced settings.

3 Click the **Start Order** tab to edit vApp startup and shutdown options.

4 Click **OK**.

Edit vApp Startup and Shutdown Options

You can change the order in which virtual machines and nested vApps within a vApp start up and shut down. You can also specify delays and actions performed at startup and shutdown.

Required privilege: **vApp.vApp application configuration**

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 In the **Start Order** tab of the Edit vApp Settings window, select a virtual machine and use the arrow keys to change the startup order.

Virtual Machines and vApps with the same start order (or within the same grouping) will start concurrently with each other.

The reverse order will be used for shutdown.

3 Select the startup and shutdown action for each virtual machine.

4 (Optional) Use the arrow keys to change the time delay for startup and shutdown for each virtual machine.

5 Click **OK**.

Edit vApp Resources

You can edit the CPU and memory resource allocation for the vApp.

Required privilege: **vApp.vApp application configuration**

Reservations on vApps and all their child resource pools, child vApps, and child virtual machines count against the parent resources only when they are powered on.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **Resources** in the Options list.

3 Edit the CPU and memory resource allocation.

4 Click **OK**.

Edit vApp Properties

You can edit any vApp property that is defined in Advanced Property Configuration.

Required privilege: **vApp.vApp application configuration**

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **Properties** in the **Options** list.

3 Edit the vApp properties.

4 Click **OK**.

Edit IP Allocation Policy

You can edit how IP addresses are allocated for the vApp.

Prerequisites

- For automatic (transient) IP allocation to work, you must use the vSphere Client and configure an IP pool. See "Configuring IP Pools," on page 204.

Required privilege: **vApp.vApp instance configuration**.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **IP Allocation Policy** in the Options list.

3 Select an IP allocation option.

Option	Description
Fixed	IP addresses are manually configured. No automatic allocation is performed.
Transient	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.

4 Click **OK**.

Add a vService Dependency

You can add a vService dependency to a virtual machine or vApp. This dependency allows a virtual machine or vApp to request that a specific vService be available.

Procedure

1 Display the virtual machine or vApp in the inventory.

2 Power off the virtual machine or vApp.

3 Right-click the virtual machine or vApp and select **Edit Settings**.

4 Click the **vServices** tab.

5 Click **Add**.

6 In the Add Dependency wizard, select the provider for this dependency and click **Next.**

7 Enter the name and description for this dependency.

8 (Optional) If this dependency is required, select the check box and click **Next**.

   Required dependencies must be bound before powering on.

9 (Optional) If this dependency should be bound to the provider immediately, select the **Bind to provider immediately** check box, and click **Next** after the validation is complete.

   If you choose to bind this dependency now, the validation result displays. If the validation fails, you cannot complete adding the dependency. Deselect the check box to proceed.

10 Review the options and click **Finish** to create the dependency.

Edit a vService Dependency

You can edit a vService dependency name, description, and requirement.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine or vApp and select **Edit Settings**

2 From the **vServices** tab in the Edit Settings dialog box, right-click on the dependency and click **Edit**.

3 In the Dependency Properties dialog box, edit the dependency name and description.

4 Select or deselect the check box to change the required status of the dependency.

   The required check box is disabled if the virtual machine or vApp is running.

5 Select a provider for the dependency.

   When you select a provider, the description is entered containing the provider description. The validation box displays the results of the validation. If validation fails, the **OK** button is disabled until another provider or no provider is selected.

6 Click **OK**.

Remove a vService Dependency

You can remove a vService dependency from a virtual machine or vApp.

Procedure

1 In the vSphere Client inventory, right-click the virtual machine or vApp and select **Edit Settings**

2 From the **vServices** tab in the Edit Settings dialog box, select the dependency and click **Remove**.

The dependency is removed from the list.

Configure Advanced vApp Properties

You can edit and configure advanced settings, such as product and vendor information, custom properties, and IP allocation.

Required privilege: **vApp.vApp application configuration**

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **Advanced** in the Options list.

3 Set and configure the settings that appear on the summary page of the virtual machine.

vApp Setting	Description
Product Name	Product Name.
Version	vApp version.
Full Version	Full version of the vApp.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor URL	If you enter a vendor URL, a user can click the vendor name on the virtual machine summary page and go to the vendor's web page.
Application URL	If you use properties to specify the virtual machine IP address, you can enter a dynamic application URL that points to a web page exposed by running the virtual machine. If you enter a valid application URL, the state of the virtual machine changes to the **Available** link when the virtual machine begins running.

If you configure the virtual machine to use the property called *webserver_ip* and the virtual machine has a web server, you can enter `http://${webserver_ip}/` as the **Application URL**.

4 (Optional) Click **View** to test the **Product URL** and **Vendor URL**.

5 Click **Properties** to edit the custom vApp properties.

6 Click **IP Allocation** to edit the supported IP allocation schemes of this vApp.

7 Click **OK**.

Define OVF Environment Properties

You can view or modify the OVF environment properties for the vApp.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **Advanced** in the Options list.

3 Click **Properties**.

4 In Advanced Property Configuration, you can perform the following actions.

- Click **New** to add a new custom property.
- Select the property and click **Edit** to edit a property.
- Click **Delete** to delete a property.

5 Click **OK**.

Edit Advanced IP Allocation Properties

You can edit the IP allocation scheme for the vApp.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **Advanced** in the **Options** list.

3 Click **IP Allocation**.

4 In the Advanced IP Allocation dialog box, you can perform the following actions.

- Select an IP allocation scheme.
- Select the IP protocols supported by the vApp: IPv4, IPv6, or both.

5 Click **OK**.

Configuring IP Pools

IP pools provide a network identity to vApps. An IP pool is a network configuration that is assigned to a network used by a vApp. The vApp can then leverage vCenter Server to automatically provide an IP configuration to its virtual machines.

Specify an IP Address Range

You can set up an IP address range by specifying a host address range within a network.

IP pool ranges are configured with IPv4 and IPv6. vCenter Server uses these ranges to dynamically allocate IP addresses to virtual machines when a vApp is set up to use transient IP allocation.

Procedure

1 In the inventory, select the datacenter that contains the vApp.

2 In the IP Pools tab, right-click the IP pool that you want to edit and select **Properties**.

   If no IP pools appear, click **Add** to add a new IP pool.

3 In the Properties dialog box, select the IPv4 or the IPv6 tab, depending on your IP protocol.

4 Enter the **IP Subnet** and **Gateway** in their respective fields.

5 (Optional) Select the **Enable IP Pool** check box.

   Enable this setting to specify an IP address range.

6 (Optional) Enter a comma-separated list of host address ranges in the **Ranges** field.

   A range consists of an IP address, a pound sign (`#`), and a number indicating the length of the range.

   The gateway and the ranges must be within the subnet, but must exclude the gateway address.

   For example, `10.20.60.4#10, 10.20.61.0#2` indicates that the IPv4 addresses can range from 10.20.60.4 to 10.209.60.13 and 10.20.61.0 to 10.20.61.1.

7 Click **OK**.

Select DHCP

You can specify that an IPv4 or IPv6 DHCP server is available on the network.

Procedure

1 In the inventory, select the datacenter that contains the vApp you are configuring.

2 In the **IP Pools** tab, right-click the IP pool that you want to edit and select **Properties**.

   If no IP pools appear, click **Add** to add a new IP pool.

3 In the Properties dialog box, select the **DHCP** tab.

4 Select either the **IPv4 DHCP Present** or **IPv6 DHCP Present** check box to indicate that one of the DHCP servers is available on this network.

5 Click **OK**.

Specify DNS Settings

Enter the DNS settings for the vApp.

Procedure

1 In the inventory, select the datacenter that contains the vApp you are configuring.

2 In the IP Pools tab, right-click the IP pool that you want to edit and select **Properties**.

If no IP pools appear, click **Add** to add a new IP pool.

3 In the Properties dialog box, select the **DNS** tab.

4 Enter the DNS server information.

Specify the servers by IP addresses separated by a comma, semicolon, or space.

You can enter the following types of DNS information:

- DNS Domain
- Host Prefix
- DNS Search Path
- IPv4 DNS Servers
- IPv6 DNS Servers

5 Click **OK**.

Specify a Proxy Server

Specify a HTTP proxy server for the vApp.

Procedure

1 In the inventory, select the datacenter that contains the vApp.

2 In the IP Pools tab, right-click the IP pool that you want to edit and select **Properties**.

If no IP pools appear, click **Add** to add a new IP pool.

3 In the Properties dialog box, select the **Proxy** tab.

4 Enter the server name and port number for the proxy server.

The server name can optionally include a colon and a port number.

For example, `web-proxy:3912` is a valid proxy server.

5 Click **OK**.

Select Network Associations

You can associate one or more networks with an IP pool.

Procedure

1 In the inventory, select the datacenter that contains the vApp.

2 In the **IP Pools** tab, right-click the IP pool that you want to edit and select **Properties**.

If no IP pools appear, click **Add** to add a new IP pool.

3 In the Properties dialog box, select the **Associations** tab.

4 Select the networks that use this IP pool.

   A network can be associated with one IP pool at a time.

5 Click **OK**.

Edit vApp Annotation in the vSphere Client

You can add or edit notes for a particular vApp.

Procedure

1 Select the vApp in the inventory.

2 Click the **Summary** tab for the vApp.

3 In the Annotation section, click **Edit**.

4 Type your comments in the Edit Service Annotation window.

5 Click **OK**.

Your comments appear under Annotation.

Monitoring Solutions with the vCenter Solutions Manager 18

A vSphere administrator uses the vCenter Solutions Manager in the vSphere Client to view the installed solutions, view detailed information about the solutions, and monitor the solution health status. You can also perform those tasks in the vSphere Web Client.

You can monitor and manage vSphere solutions from the vSphere Client or the vSphere Web Client. Both clients display an inventory of vSphere solutions and details about each solution.

A solution is an extension of the vCenter Server that adds new functions to a vCenter Server instance. For example, vSphere ESX Agent Manager is a standard vCenter solution provided by VMware that allows you to manage ESX host agents that add new capabilities to ESX hosts. Another standard solution that vSphere provides is vService Manager. VMware products that integrate with vCenter Sever are also considered solutions. You can install a solution to add functionality from third-party technologies to the standard functions of vCenter Server. Solutions typically are delivered as OVF packages. You can install and deploy solutions from vSphere Client. Solutions can be integrated into the vCenter Solutions Manager.

If a virtual machine or vApp is running a solution, a custom icon appears next to it in the inventory view of the vSphere Client. When you power on or power off a virtual machine or vApp, you are notified that you are performing this operation on an entity that is managed by the solution manager.

Each solution registers a unique icon to identify that the virtual machine or vApp is being managed by that solution. The icons show the power states (powered on, paused, powered off).

The solutions display more than one type of icon if they manage more than one type of virtual machine or vApp.

When you attempt an operation on a virtual machine or a vApp that is managed by a solution, an informational warning message appears.

For more information, see the *Developing and Deploying vSphere Solutions, vServices, and ESX Agents* documentation.

This chapter includes the following topics:

- "Viewing Solutions," on page 208
- "Monitoring Agents," on page 208
- "Monitoring vServices," on page 209

Viewing Solutions

You can deploy, monitor, and interact with solutions that are installed in a vCenter Server instance with the vCenter Solutions Manager. The Solutions Manager displays information about the health of a solution.

You can navigate to the Solutions Manager from the home page of the vSphere Client. The Solutions Manager view displays information about the solution:

- Solution name
- Solution health
- vService providers

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Click the Solutions Manager icon from vSphere Client home.

2 Navigate through the tabs in the Solutions Manager.

   - **Summary** tab. Lists the number of installed solutions and a brief health overview for each of the solutions.
   - **Solutions** tab. Lists each managed solution.
   - **Health** tab. Provides the health status of the vCenter services. It also shows alerts or warnings for each of the services.

3 In the Solutions Manager inventory, click one of the solutions.

   - **Summary** tab. Lists information about the solution, including a link to the product and vendor Web sites, a link to launch the management UI in a separate window, and a link to the virtual machine or vApp running this solution.

     Selecting the vendor Web site link takes you to the Summary page of the virtual machine or vApp. A link under "Managed by" returns you to the solution.
   - **Virtual Machines** tab. Lists all the virtual machines belonging to the solution
   - **vServices Providers** tab.
   - **Management** tab or any other tabs the solution specified.

Monitoring Agents

The vCenter Solutions Manager displays the vSphere ESX Agent Manager agents that you use to deploy and manage related agents on ESX/ESXi hosts.

You can use the Solutions Manager to keep track of whether the agents of a solution are working as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and a list of issues.

When the status of a solution changes, the Solutions Manager updates the ESX Agent Manager summary status and state. Administrators use this status to track whether the goal state is reached.

The agent health status is indicated by a specific color.

Table 18-1. ESX Agent Manager health status

Status	Description
Red	The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution, and the solution alerts the administrator to power on the agent.
Yellow	The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.
Green	A solution and all its agents have reached the goal state.

Monitoring vServices

A vService is a service or function that a solution provides to virtual machines and vApps. A solution can provide one or more vServices. These vServices integrate with the platform and are able to change the environment in which the vApp or virtual machine runs.

A vService is a type of service for a virtual machine and a vApp provided by a vCenter extension. Virtual machines and vApps can have dependencies on vServices. Each dependency is associated with a vService type. The vService type must be bound to a particular vCenter extension that implements that vService type. This vService type is similar to a virtual hardware device. For example, a virtual machine can have a networking device that at deployment must be connected to a particular network.

The vService Manager allows a solution to connect to operations related to OVF templates:

- Importing OVF templates. Receive a callback when OVF templates with a vService dependancy of a certain type is imported.
- Exporting OVF templates. Inserts OVF sections when a virtual machine is exported.
- OVF environment generation. Inserts OVF sections into the OVF environment at the power-on instance.

The **vServices** tab in the Solution Manager provides details for each vCenter extension. This information allows you to monitor vService providers and list the virtual machines or vApps to which they are bound.

Using Host Profiles in the vSphere Client 19

The host profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host or cluster in vCenter Server.

Host profiles eliminates per-host, manual, or UI-based host configuration and maintains configuration consistency and correctness across the datacenter by using host profile policies. These policies capture the blueprint of a known, validated reference host configuration and use this to configure networking, storage, security, and other settings on multiple hosts or clusters. You can then check a host or cluster against a profile's configuration for any deviations.

This chapter includes the following topics:

- "Host Profiles Usage Model," on page 211
- "Access Host Profiles View," on page 212
- "Creating a Host Profile," on page 212
- "Export a Host Profile," on page 213
- "Import a Host Profile," on page 214
- "Clone a Host Profile," on page 214
- "Edit a Host Profile," on page 214
- "Manage Profiles," on page 217
- "Checking Compliance," on page 220
- "Host Profiles and vSphere Auto Deploy," on page 222

Host Profiles Usage Model

You perform host profiles tasks in a certain workflow order.

You must have an existing vSphere installation with at least one properly configured host.

1. Set up and configure the host that will be used as the reference host.

   A reference host is the host from which the profile is created.

2. Create a profile using the designated reference host.
3. Attach a host or cluster to the profile.
4. Check the host's compliance to the reference host's profile. If all hosts are compliant with the reference host, they are correctly configured.
5. Apply the host profile of the reference host to other hosts or clusters of hosts.

Using host profiles is only supported for VMware vSphere 4.0 hosts or later. This feature is not supported for VMware Infrastructure 3.5 or earlier hosts. If you have VMware Infrastructure 3.5 or earlier hosts managed by your vCenter Server 4.0 or later, the following problems can occur if you try to use host profiles for those hosts:

- You cannot create a host profile that uses a VMware Infrastructure 3.5 or earlier host as a reference host.
- You cannot apply a host profile to any VMware Infrastructure 3.5 or earlier hosts. The compliance check fails.
- While you can attach a host profile to a mixed cluster that contains VMware Infrastructure 3.5 or earlier hosts, the compliance check for those earlier hosts fails.

As a licensed feature of vSphere, host profiles are only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate vSphere licensing for your hosts.

If you want the host profile to use directory services for authentication, the reference host needs to be configured to use a directory service. See the *vSphere Security* documentation.

Hosts Provisioned with vSphere® Auto Deploy

For hosts provisioned with vSphere Auto Deploy, vCenter Server owns the entire host configuration, which is captured in a host profile. In most cases, the host profile information is sufficient to store all configuration information. Sometimes the user is prompted for input when the host provisioned with Auto Deploy boots. The answer file mechanism manages those cases. See the *vSphere Installation and Setup* documentation.

Access Host Profiles View

The Host Profiles main view lists all available profiles. Administrators can also use the Host Profiles main view to perform operations on host profiles and configure profiles.

The Host Profiles main view should be used by experienced administrators who wish to perform host profile operations and configure advanced options and policies. Most operations such as creating new profiles, attaching entities, and applying profiles can be performed from the Hosts and Clusters view.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

◆ Select **View > Management > Host Profiles**.

Any existing profiles are listed on the left side in the profiles list. When a profile is selected from the profile list, the details of that profile are displayed on the right side.

Creating a Host Profile

You create a new host profile by using the designated reference host's configuration.

A host profile can be created from:

- Host Profile main view
- host's context menu

Create a Host Profile from Host Profiles View

You can create a host profile from the Host Profiles main view using the configuration of an existing host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

You must have a vSphere installation and at least one properly configured host in the inventory.

Procedure

1 In the Host Profiles main view, click **Create Profile**.

The Create Profile wizard appears.

2 Select the option to create a new profile and click **Next**.

3 Select the host you want to designate as the reference host for the new host profile and click **Next**.

The reference host must be a valid host.

4 Type the name and enter a description for the new profile and click **Next**.

5 Review the summary information for the new profile and click **Finish** to complete creating the profile.

The new profile appears in the profile list.

Create a Host Profile from Host

You can create a new host profile from the host's context menu in the Hosts and Clusters inventory view.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

You must have a vSphere installation and at least one properly configured host in the inventory.

Procedure

1 In the Host and Clusters view, select the host that you want to designate as the reference host for the new host profile.

The host must be a valid host to use as a reference host.

2 Right-click the host and select **Host Profile > Create Profile from Host**

The Create Profile from Host wizard opens.

3 Type the name and enter a description for the new profile and click **Next**.

4 Review the summary information for the new profile and click **Finish** to complete creating the profile.

The new profile appears in the host's Summary tab.

Export a Host Profile

You can export a profile to a file that is in the VMware profile format (`.vpf`).

Note When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

Procedure

1 In the Host Profiles view page, select the profile to export from the profile list.

2 Right-click the profile and select the **Export Profile**.

3 Select the location and type the name of the file to export the profile.

4 Click **Save**.

Import a Host Profile

You can import a profile from a file in the VMware profile format (`.vpf`).

NOTE When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

Procedure

1 In the Host Profiles main view, click the **Create Profile** icon.

The Create Profile wizard appears.

2 Select the option to import a profile and click **Next**.

3 Enter or browse the VMware Profile Format file to import and click **Next**.

4 Select a valid host you want to designate as the reference host for the imported profile and click **Next**.

5 Type the name, enter a description for the imported profile, and click **Next** when finished.

6 Review the summary information for the imported profile and click **Finish** to complete importing the profile.

The imported profile appears in the profile list.

Clone a Host Profile

A host profile clone is a copy of an existing host profile.

Procedure

1 In the Host Profiles main view, select the profile to clone.

2 Click **Clone Profile**.

3 A clone of the profile appears in the Host Profiles view.

Edit a Host Profile

You can view and edit host profile policies, select a policy to be checked for compliance, and change the policy name or description.

Procedure

1 In the Host Profiles main view, select the profile to edit from the profile list.

2 Click **Edit Host Profile**.

3 (Optional) Change the profile name or description in the fields at the top of the Profile Editor.

4 Edit the policy.

5 (Optional) Enable or disable the policy compliance check.

6 Click **OK** to close the Profile Editor.

Edit a Policy

A policy describes how a specific configuration setting should be applied. The Profile Editor allows you to edit policies belonging to a specific host profile.

On the left side of the Profile Editor, you can expand the host profile. Each host profile is composed of several subprofiles that are designated by functional group to represent configuration instances. Each subprofile contains many policies and compliance checks that describe the configuration that is relevant to the profile. You can configure certain subprofiles, example policies, and compliance checks.

Each policy consists of one or more options that contains one or more parameters. Each parameter consists of a key and a value. The value can be one of a few basic types, for example integer, string, string array, or integer array.

Table 19-1. Subset of Host Profile Subprofile Configurations

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Memory reservation	Set memory reservation to a fixed value.	
Storage	Configure storage options, including Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA), FCoE and iSCSI adapters, and NFS storage.	■ Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host first, and then extract the host profile from that host. If you use the Profile Editor to edit the policies, to avoid compliance failures, make sure that you thoroughly understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information on the NMP and PSA, see the *vSphere Storage* documentation. ■ Setting values for the Initiator IPv6 Address and Initiator IPv6 Prefix options in a host profile with independent hardware iSCSI adapters has no effect on the HBA because no independent iSCSi HBAs have IPv6 support. ■ Add the rules that change device attributes before extracting the host profile from the reference host. After attaching a host to the host profile, if you edit the profile and change the device attributes (for example, mask device paths or adding SATP rules to mark the device as SSD) you are prompted to reboot the host in order to make the changes. However, after rebooting compliance failures occur because the attributes changed. Because Host Profiles extract device attributes before rebooting, if any changes occur after the reboot, it evaluates and finds those changes, and reports it as non-compliant.
Networking	Configure virtual switch, port groups, physical NIC speed, security and NIC teaming policies, vSphere Distributed Switch, and vSphere Distributed Switch uplink port.	When DHCPv6 is enabled in the networking sub-profile, the corresponding ruleset must also be manually turned on in the firewall subprofile.

Table 19-1. Subset of Host Profile Subprofile Configurations (Continued)

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Date and Time	Configure the time settings and timezone of server.	For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone. The default time zone is set to the local time and location of the vSphere Client machine. Network Time Protocol (NTP) should be correctly configured. You can configure the NTP settings on the host's configuration tab. Click **Time Configuration**, then Properties at the top right of the panel.
Firewall	Enable or disable a ruleset.	
Security	Add a user or a usergroup and set the root password.	
Service	Configure settings for a service.	
Advanced	Modify advanced options.	■ Host Profiles do not check advanced settings if they are the same as the default settings. vCenter Server only copies the advanced configuration settings that have changed and differ from the default values. In addition, compliance checks are limited to only the settings that are copied. ■ Host Profiles does not support the configuration of PCI devices for virtual machine passthrough on the ESXi host.

Other profile configuration categories include: user group, authentication, kernel module, DCUI keyboard, host cache settings, SFCB, resource pools, login banner, SNMP agent, power system, and CIM indication subscriptions.

Procedure

1 Open the Profile Editor for the profile to edit.

2 On the left side of the Profile Editor, expand a subprofile until you reach the policy to edit.

3 Select the policy.

   On the right side of the Profile Editor, the policy options and parameters are displayed on the **Configuration Details** tab.

4 Select a policy option from the drop-down menu and set its parameter.

5 Click **OK** when you are finished editing the profile.

   Note The change is made when the "Update host profile" task is completed in the Recent Tasks status. If you attempt to apply the profile before the task is complete, the profile configuration does not contain the change.

6 (Optional) If you make a change to a policy, but want to revert back to the default option, click **Revert** and the option is reset.

Enable Compliance Check

You can decide whether a host profile policy is considered during compliance check.

Procedure

1 Open the Profile Editor for a profile and navigate to the policy you wish to enable for compliance check.

2 On the right side of the Profile Editor, select the **Compliance Details** tab.

3 Enable the check box for the policy.

NOTE The check box is enabled by default. If you disable the check box so this policy is not checked for compliance, the other policies that are enabled for compliance check will still be checked.

Manage Profiles

After you create a host profile, you can manage the profile by attaching a profile to a particular host or cluster and then applying that profile to the host or cluster.

You can associate a profile and a host or cluster either by attaching the profile to the host or cluster, or by attaching the host or cluster to the profile. You can then apply the profile to the host or cluster.

NOTE A host profile must have a valid reference host associated with it before you can manage the profile.

Attaching Host or Cluster Entities to a Host Profile

If you want to set up a host to use the same configuration as a reference host, you can attach the host to a profile. You can also attach a cluster to a profile.

Profiles can also be attached to a cluster. In order to be compliant, all hosts within an attached cluster must be configured according to the profile. Hosts are not automatically configured in accordance to the host profile that is attached with the cluster when it is added to the cluster. When a host is added to a cluster that is attached to a profile, the host is automatically attached to the profile.

You can attach a host or cluster to a profile from:

- Host Profiles main view
- Host's context menu
- Cluster's context menu
- Cluster's Profile Compliance tab

Attach Entities from the Host Profiles View

Before you can apply the profile to an entity (host or cluster of hosts), you need to attach the entity to the profile or the profile to the entity.

You can attach a host or cluster to a profile from the Host Profiles main view.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remains.

Procedure

1 In the Host Profiles main view, select the profile to which you want to add the host or cluster from the profile list.

2 Click the **Attach Host/Cluster** icon.

3 Select the host or cluster from the expanded list and click **Attach**.

   The host or cluster is added to the Attached Entities list.

4 Click **OK** to close the dialog.

Attach Profiles from the Host

Before you can apply the profile to a host you need to attach the host to the profile or the profile to the host.

You can attach a profile to a host from the host's context menu in the Hosts and Clusters inventory view.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remain.

Procedure

1 In the Host and Clusters view, select the host to which you want to attach a profile.

2 Right-click the host and select **Host Profile > Manage Profile**.

   NOTE If no host profiles exist in your inventory, a dialog appears asking if you want to create and attach the host to this profile.

3 In the Attach Profile dialog, select the profile to attach to the host and click **OK**.

The host profile is updated in the **Summary** tab of the host.

Applying Profiles

To bring a host to the desired state as specified in the profile, apply the profile to the host.

You can apply a profile to a host from:

- Host Profiles main view
- Host's context menu
- Cluster's Profile Compliance tab

If the profile is not applied, or configured to what is specified in the profile, it will cause the compliance status for the profile to fail the next time a compliance check is performed. You fix this by applying the profile to the host.

Apply a Profile from the Host Profiles View

You can apply a profile to a host from the Host Profiles main view.

Prerequisites

The profile must be attached to the host and the host must be in maintenance mode before a profile is applied to it.

Procedure

1 In the Host Profiles main view, select the profile you want to apply to the host.

2 Select the **Hosts and Clusters** tab.

   The list of attached hosts are shown under Entity Name.

3 Click **Apply Profile**.

   In the Profile Editor, you might be prompted to enter the required parameters needed to apply the profile.

4 Enter the parameters and click **Next**.

5 Continue until all the required parameters are entered.

6 Click **Finish**.

Compliance Status is updated.

Apply a Profile from the Host

You can apply a profile to a host from the host's context menu.

Prerequisites

The host must be in maintenance mode before a profileis applied to it.

Procedure

1 In the Host and Clusters view, select the host to which you want to apply a profile.

2 Right-click the host and select **Host Profile > Apply Profile**.

3 In the Profile Editor, enter the parameters and click **Next**.

4 Continue until all the required parameters are entered.

5 Click **Finish**.

Compliance Status is updated.

Change Reference Host

The reference host configuration is used to create the host profile.

You can perform this task from the Host Profiles main view or from the host's context menu.

Prerequisites

The host profile must already exist.

Procedure

1 In the Host Profiles main view, right-click the profile you wish to change the reference host and select **Change Reference Host**.

2 Expand the inventory list and select the host you want to use as the new reference host for the profile.

3 Click **Update**.

   The **Reference Host** is updated.

4 Click **OK**.

The Summary tab for the host profile lists the updated reference host.

Manage Profiles from a Cluster

You can create a profile, attach a profile, or update reference hosts from the cluster's context menu.

Procedure

◆ In the Hosts and Clusters view, right-click a cluster and select **Host Profile > Manage Profile**. Depending on your host profile setup, one of the following results occurs:

Profile Status and Task	Result
If the cluster is not attached to a host profile and no profile exist in your inventory, create a profile.	a A dialog box opens asking if you would like to create a profile and attach it to the cluster. b If you select **Yes**, the Create Profile wizard opens.
If the cluster is not attached to a host profile and one or more profiles exist in your inventory, attach a profile.	a The Attach Profile dialog opens. b Select the profile you want to attach to the cluster and click **OK.**
If the cluster is already attached to a host profile, detach a profile or attach to a different profile.	In the dialog box, click **Detach** to detach the profile from the cluster or **Change** to attach a different profile to the cluster.

Updating Profiles From the Reference Host

If the configuration of the host from which a profile was created (the reference host) changes, you can update the local profile so that the local host configuration matches the reference host's configuration.

Once you create a host profile, you might need to make incremental updates to the profile. You can do this using two methods:

- Make the configuration changes to the reference host in the vSphere Client, then update the profile from the reference host. The settings within the existing profile are updated to match those of the reference host.
- Update the profile directly using the Profile Editor.

While updating the profile from the Profile Editor can be more comprehensive and provide more options, updating the profile from the reference host allows you to validate the configuration before rolling it out to other hosts that are attached to the profile.

Updating the profile from the reference host is performed from the Host Profiles main view.

Procedure

◆ In the Host Profiles main view, right-click the profile you want to update and select **Update Profile From Reference Host**.

Checking Compliance

Checking compliance ensures that the host or cluster continues to be correctly configured.

After a host or cluster is configured with the reference host profile, a manual change, for example, can occur, making the configuration incorrect. Checking compliance on a regular basis ensures that the host or cluster continues to be correctly configured.

Check Compliance from the Host Profiles View

You can check the compliance of a host or cluster to a profile from the Host Profiles main view.

Procedure

1 From the Host Profiles list, select the profile that you want to check.

2 In the **Hosts and Clusters** tab, select the host or cluster from the list under Entity Name.

3 Click **Check Compliance Now**.

The compliance status is updated as Compliant, Unknown, or Non-compliant.

If the compliance status is Non-compliant, you can apply the the profile to the host.

Check Compliance from Host

After a profile has been attached to a host, run a compliance check from the host's context menu to verify the configuration.

Procedure

1 In the Host and Clusters view, select the host on which you want to run the compliance check.

2 Right-click the host and select **Host Profile > Check Compliance**

The host's compliance status is displayed in the host's **Summary** tab.

If the host is not compliant, you must apply the profile to the host.

Check Cluster Compliance

A cluster may be checked for compliance with a host profile or for specific cluster requirements and settings.

Procedure

1 In the Host and Clusters view, select the cluster on which you want to run the compliance check.

2 In the Profile Compliance tab, click **Check Compliance Now** to check the cluster's compliance with both the host profile that is attached to this cluster and the cluster requirements, if any.

- The cluster is checked for compliance with specific settings for hosts in the cluster, such as DRS, HA, and DPM. For example, it may check if vMotion is enabled. The compliance status for the cluster requirements is updated. This check is performed even if a host profile is not attached to the cluster.
- If a host profile is attached to the cluster, the cluster is checked for compliance with the host profile. The compliance status for the host profile is updated.

3 (Optional) Click **Description** next to the Cluster Requirements for a list of the specific cluster requirements.

4 (Optional) Click **Description** next to Host Profiles for a list of the specific host profile compliance checks.

5 (Optional) Click **Change** to change the host profile that is attached to the cluster.

6 (Optional) Click **Remove** to detach the host profile that is attached to the cluster.

If the cluster is not compliant, the profile must be applied separately to each host within the cluster.

Host Profiles and vSphere Auto Deploy

Host profiles are used to help vSphere Auto Deploy provision physical ESXi hosts with configuration state information (virtual switches, driver settings, boot parameters, and so on).

Configuration state information cannot be stored directly on a host provisioned with Auto Deploy. Instead, you can create a reference host and configure it with the settings you want. Then, create a host profile using this reference host. Auto Deploy can apply the host profile to these hosts so they are configured with these settings, or you can apply the host profile using the client.

To apply a host profile to a host, the host must be placed into maintenance mode. The user is prompted to type answers for policies that are specified during host profile creation when the host profile is applied.

A host provisioned with Auto Deploy can be rebooted while the host profile is attached to the host. After rebooting, values stored in the answer file help the host provisioned with Auto Deploy to apply the profile. An answer file is created that contains a series of key value pairs for the user input options.

The answer file contains the user input policies for a host profile. The file is created when the profile is initially applied to a particular host.

NOTE If you deploy ESXi through host profiles, configure syslog to store logs on a remote server. See "Set up Syslog from the Host Profiles Interface" in the *Installation and Setup* documentation for instructions.

See "Setting up an Auto Deploy Reference Host" in the vSphere Auto Deploy documentation for more information.

Check Answer File Status

The answer file status indicates the state of the answer file. The status of an answer file can be complete, incomplete, missing, or unknown.

Prerequisites

The answer file status can only be checked when the host profile is atached to a host.

Procedure

- In the host profiles view, click **Check Answer File**.

The Answer File Status for the host profile is updated. The status indicates one of the following states:

Incomplete	The answer file is missing some of the required user input answers.
Complete	The answer file has all of the user input answers needed.
Unknown	The host and associated profile exist but the status of the answer file is not known. This is the initial state of an answer file.

Update Answer File

You can update or change the user input parameters for the host profiles policies in the answer file.

Procedure

1. Right-click the host entity and select **Update Answer File**.
2. When prompted, enter or change the user input parameter, and click **Next**.
3. Click **Update** when finished entering changes.

Import Answer File

You can import a previously exported answer file to associate with a host profile.

Prerequisites

The imported answer file must be associated with at least one host.

Procedure

1 Right-click the host entity and select **Import Answer File**.

2 Select the answer file to import.

Export Answer File

You can export an answer file so that it can be imported and used by another host profile.

The answer file might contain sensitive information such as passwords and IP addresses. If exported, this information is vulnerable to unauthorized access. During the export process all passwords are removed from the answer file. When the answer file is imported, the password information must be re-entered.

Procedure

1 Right-click the host entity and select **Export Answer File**.

2 Select the location to save the answer file.

Networking in the vSphere Client 20

When you connect directly to a host or vCenter Server with the vSphere Client, you can view and configure vSphere standard switches.

This chapter includes the following topics:

- "Networking Limitations in the vSphere Client," on page 225
- "View Networking Information in the vSphere Client," on page 226
- "View Network Adapter Information in the vSphere Client," on page 226
- "Setting Up Networking with vSphere Standard Switches," on page 227
- "Setting Up Networking with vSphere Distributed Switches," on page 230

Networking Limitations in the vSphere Client

The network tasks that you can perform when you connect directly to an ESXi host or vCenter Server system with the vSphere Client are limited.

The following network features are unavailable or read-only in the vSphere Client:

- vSphere vMotion across vCenter Server systems
- vSphere vMotion across large geographical distances
- Network DRS
- DRS anti-affinity rules
- Network I/O control
- Open vSwitch
- Proxy switch autoscale capability
- Opaque networks
- SR-IOV
- LACP
- Multicast
- Multi-instance TCP/IP stack and upgrade
- IPv6 support for ESX architecture, NFS 4.1 storage operations, iSCSI, guest OS customizations, virtual datacenters

Use the vSphere Web Client as the primary interface for managing the full range of network functions available in your vSphere 6.0 environment.

View Networking Information in the vSphere Client

The vSphere Client shows general networking information and information specific to network adapters.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 (Optional) Choose the type of networking to view.

Option	Description
vSphere Standard Switch	Displays vSphere standard switch networking on the host.
vSphere Distributed Switch	Displays vSphere distributed switch networking on the host.

The **vSphere Distributed Switch** option appears only on hosts that are connected to one or more vSphere distributed switches.

Networking information is displayed for each virtual switch on the host.

View Network Adapter Information in the vSphere Client

For each physical network adapter on the host, you can view information such as the speed, duplex, and observed IP ranges.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 Click the **Configuration** tab, and click **Network Adapters**.

The network adapters panel shows the following information.

Table 20-1. Network Adapter Parameters

Option	Description
Device	Name of the network adapter.
Speed	Actual speed and duplex of the network adapter.
Configured	Configured speed and duplex of the network adapter.
Switch	vSphere standard switch or vSphere distributed switch that the network adapter is associated with.
MAC Address	MAC Address of the network adapter.
Observed IP ranges	IP addresses that the network adapter is likely to have access to.
Wake on LAN supported	Network adapter ability to support Wake on the LAN.

Setting Up Networking with vSphere Standard Switches

vSphere standard switches handle network traffic at the host level in a vSphere deployment.

Add a Virtual Machine Port Group

Virtual machine port groups provide networking for virtual machines.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Select the vSphere Standard Switch view.

Standard switches appear in an overview that includes a detailed layout.

4 On the right side of the page, click **Add Networking**.

5 Accept the default connection type, **Virtual Machine**, and click **Next**.

6 Select **Create a vSphere standard switch** or one of the listed existing standard switches and the associated physical adapters to use for this port group.

You can create a standard switch with or without Ethernet adapters.

If you create a standard switch without physical network adapters, all traffic on that switch is confined to that switch. No other hosts on the physical network or virtual machines on other standard switches can send or receive traffic over this standard switch. You might create a standard switch without physical network adapters if you want a group of virtual machines to be able to communicate with each other, but not with other hosts or with virtual machines outside the group.

7 Click **Next**.

8 In the Port Group Properties group, enter a network label that identifies the port group that you are creating.

Use network labels to identify migration-compatible connections common to two or more hosts.

9 (Optional) If you are using a VLAN, for **VLAN ID**, enter a number between 1 and 4094.

If you enter 0 or leave the option blank, the port group detects only untagged (non-VLAN) traffic. If you enter 4095, the port group can detect traffic on any VLAN while leaving the VLAN tags intact.

10 Click **Next**.

11 After you determine that the switch is configured correctly, click **Finish**.

Set Up VMkernel Networking on a vSphere Standard Switch

Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 In the vSphere Standard Switch view, click **Add Networking**.

4 Select **VMkernel** and click **Next**.

5 Select the vSphere standard switch to use, or select **Create a vSphere standard switch** to create a new vSphere standard switch.

6 Select the check boxes for the network adapters for your vSphere standard switch to use.

Select adapters for each vSphere standard switch so that virtual machines or other services that connect through the adapter can reach the correct Ethernet segment. If no adapters appear under Create a new vSphere standard switch, all the network adapters in the system are being used by existing vSphere standard switches or vSphere distributed switches. You can either create a vSphere standard switch without a network adapter, or select a network adapter that an existing vSphere standard switch uses.

7 Click **Next**.

8 Select or enter a network label and a VLAN ID.

Option	Description
Network Label	A name that identifies the port group that you are creating. This is the label that you specify when you configure VMkernel services such as vMotion and IP storage and you configure a virtual adapter to be attached to this port group.
VLAN ID	Identifies the VLAN that the port group's network traffic will use.

9 (Optional) Select **Use this port group for vMotion** to enable this port group to advertise itself to another host as the network connection through which vMotion traffic should be sent.

10 (Optional) Select **Use this port group for fault tolerance logging**.

11 (Optional) Select **Use this port group for management traffic**.

12 If IPv6 is enabled on the host, select **IP (Default)**, **IPv6**, or **IP and IPv6 networking**.

This option does not appear on hosts that do not have IPv6 enabled. IPv6 configuration cannot be used with dependent hardware iSCSI adapters.

13 Click **Next**.

14 Select how to obtain IP settings.

Option	Description
Obtain IP settings automatically	Use DHCP to obtain IP settings.
Use the following IP settings	Specify IP settings manually. a Enter the IP address and subnet mask for the VMkernel interface. b Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI. On the **DNS Configuration** tab, the name of the host is entered by default. The DNS server addresses that were specified during installation are also preselected, as is the domain. c Click **OK** and click **Next**.

15 If you are using IPv6 for the VMkernel interface, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisement to obtain IPv6 addresses.
Static IPv6 addresses	a Click **Add** to add a new IPv6 address. b Enter the IPv6 address and subnet prefix length, and click **OK**. c To change the VMkernel default gateway, click **Edit**.

16 Click **Next**.

17 Review the information, click **Back** to change any entries, and click **Finish**.

View VMkernel Routing Information on a vSphere Standard Switch

You can view IP and IPv6 routing information, such as network, prefix, and gateway, for a VMkernel network interface on a vSphere standard switch.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 Click **Properties** for the standard switch associated with the VMkernel interface to view.

3 On the Ports tab, select the VMkernel network adapter to view, and click **View Routing Table** under IP Settings or IPv6 Settings.

A routing table that includes network, prefix, and gateway information for the selected VMkernel network adapter appears.

Change the Number of Ports for a vSphere Standard Switch

A vSphere standard switch serves as a container for port configurations that use a common set of network adapters, including sets that contain no network adapters at all. Each virtual switch provides a finite number of ports through which virtual machines and network services can reach one or more networks.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 On the right side of the page, click **Properties** for the standard switch that you want to edit.

4 Click the **Ports** tab.

5 Select the standard switch item in the Configuration list, and click **Edit**.

6 Click the **General** tab.

7 Choose the number of ports that you want to use from the drop-down menu.

8 Click **OK**.

What to do next

Changes will not take effect until the system is restarted.

Change the Speed of an Uplink Adapter

You can change the connection speed and duplex of an uplink adapter.

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select a standard switch and click **Properties**.

4 Click the **Network Adapters** tab.

5 To change the configured speed and duplex value of a network adapter, select the network adapter and click **Edit**.

6 To select the connection speed manually, select the speed and duplex from the drop-down menu.

   Choose the connection speed manually if the NIC and a physical switch might fail to negotiate the proper connection speed. Symptoms of mismatched speed and duplex include low bandwidth or no link connectivity.

   The adapter and the physical switch port it is connected to must be set to the same value, such as auto and auto or ND and ND, where ND is some speed and duplex, but not auto and ND.

7 Click **OK**.

Add Uplink Adapters

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

Procedure

1 Log in to the ESXi host using the vSphere Client and select the host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select a standard switch and click **Properties**.

4 Click the **Network Adapters** tab.

5 Click **Add** to launch the Add Adapter wizard.

6 Select one or more adapters from the list and click **Next**.

7 (Optional) To reorder the NICs into a different category, select a NIC and click **Move Up** and **Move Down**.

Option	Description
Active Adapters	Adapters that the standard switch uses.
Standby Adapters	Adapters that become active if one or more of the active adapters fails.

8 Click **Next**.

9 Review the information on the Adapter Summary page, click **Back** to change any entries, and click **Finish**.

   The list of network adapters reappears, showing the adapters that the standard switch now claims.

10 Click **Close** to exit the dialog box.

   The Networking section in the **Configuration** tab shows the network adapters in their designated order and categories.

Setting Up Networking with vSphere Distributed Switches

With vSphere distributed switches you can set up and configure networking in a vSphere environment.

Add a vSphere Distributed Switch

Create a vSphere distributed switch on a vCenter Server datacenter to handle networking traffic for all associated hosts on the datacenter.

If your system has complex port group requirements, create a distributed port group rather than a default port group.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 In the vSphere Client, select the Networking inventory view and select the datacenter.

2 Select **Inventory > Datacenter > New vSphere Distributed Switch**.

3 Select a vSphere distributed switch version.

Option	Description
vSphere Distributed Switch Version: 4.0	Compatible with ESX/ESXi version 4.0 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 4.1.0	Compatible with ESX/ESXi version 4.1 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 5.0.0	Compatible with ESXi version 5.0 and later.
vSphere Distributed Switch Version: 5.1.0	Compatible with ESXi version 5.1 and later. eatures released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 5.5.0	Compatible with ESXi version 5.5 and later. eatures released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 6.0.0	Compatible with ESXi version 6.0 and later.

4 Click **Next**.

5 In the **Name** text box, type a name for the new vSphere distributed switch.

6 Use the arrow buttons to select the **Number of uplink ports**, and click **Next**.

Uplink ports connect the distributed switch to physical NICs on associated hosts. The number of uplink ports is the maximum number of allowed physical connections to the distributed switch per host.

7 Select whether to add hosts and their physical adapters to the vSphere distributed switch now or later.

If you select **Add now**, select the hosts and physical adapters to use by clicking the check box next to each host or adapter. You can only free physical adapters to a vSphere distributed switch during distributed switch creation.

8 (Optional) Set the maximum number of ports on a host.

a Click **View Details** for the host.

b Select the maximum number of ports for the host from the drop-down menu.

c Click **OK**.

9 Click **Next**.

10 (Optional) Select whether to **Automatically create a default port group**.

This option creates a distributed port group with default settings.

11 Click **Finish**.

What to do next

If you chose to add hosts later, you must add hosts to the distributed switch before adding network adapters.

Network adapters can be added from the host configuration page of the vSphere Client, using Manage Hosts, or by using Host Profiles.

Add Hosts to a vSphere Distributed Switch

You can add hosts and physical adapters to a vSphere distributed switch at the distributed switch level after it is created.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1. Log in to the vSphere Client and select the **Networking** inventory view.
2. Right-click the vSphere distributed switch in the inventory pane, and select **Add Host**.
3. Select the hosts to add.
4. Under the selected hosts, select the physical adapters to add and click **Next**.

   You can select physical adapters that are not being used and physical adapters that are being used.

   NOTE Moving a physical adapter to a distributed switch without moving any associated virtual adapters can cause those virtual adapters to lose network connectivity.

5. For each virtual adapter, select **Destination port group** and select a port group from the drop-down menu to migrate the virtual adapter to the distributed switch or select **Do not migrate**.
6. (Optional) Set the maximum number of ports on a host.
   a. Click **View Details** for the host.
   b. Select the maximum number of ports for the host from the drop-down menu.
   c. Click **OK**.
7. Click **Next**.
8. (Optional) Migrate virtual machine networking to the distributed switch.
   a. Select **Migrate virtual machine networking**.
   b. For each virtual machine, select **Destination port group** and select a port group from the drop-down menu or select **Do not migrate**.
9. Click **Next**.
10. (Optional) If you need to make any changes, click **Back** to the appropriate screen.
11. Review the settings for the distributed switch and click **Finish**.

Manage Hosts on a vSphere Distributed Switch

You can change the configuration for hosts and physical adapters on a vSphere distributed switch after they are added to the distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1. Log in to the vSphere Client and select the **Networking** inventory view.
2. Right-click the distributed switch and select **Manage Hosts**.
3. Select the hosts to manage and click **Next**.
4. Select the physical adapters to add, deselect the physical adapters to remove, and click **Next**.
5. For each virtual adapter, select the **Destination port group** from the drop-down menu to migrate the virtual adapter to the distributed switch or select **Do not migrate**.
6. Click **Next**.
7. Migrate virtual machine networking to the vSphere distributed switch.
   a. Select **Migrate virtual machine networking**.
   b. For each virtual machine, select the **Destination port group** from the drop-down menu or select **Do not migrate**.
8. Click **Next**.
9. (Optional) If you need to make any changes, click **Back** to the appropriate screen.
10. Review the settings for the distributed switch, and click **Finish**.

Set the Number of Ports Per Host on a vSphere Distributed Switch

Set the maximum number of ports on a host to limit the number of distributed ports that can exist on one or more hosts associated with a vSphere distributed switch.

Procedure

1. Log in to the vCenter Server system using the vSphere Client.
2. Select the host to modify in the inventory pane.
3. On the host **Configuration** tab, click **Networking**.
4. Select the **vSphere Distributed Switch** view.
5. Click **Properties** next to the vSphere distributed switch to modify.
6. Select the maximum number of ports from the drop-down menu, and click **OK**.

What to do next

If you are changing the maximum number of ports for a host after the host is added to the distributed switch, you must restart the host before the new maximum takes effect.

Edit General vSphere Distributed Switch Settings

You can edit the general settings for a vSphere distributed switch, such as the distributed switch name and the number of uplink ports on the distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select **General** to edit the vSphere distributed switch settings.

Option	Description
Name	Type the name for the distributed switch.
Number of Uplink Ports	Select the number of uplink ports for the distributed switch.
Notes	Type any notes for the distributed switch.

4 (Optional) Edit uplink port names.

   a Click **Edit uplink names**.

   b Type new names for one or more uplink ports.

   c Click **OK**.

5 Click **OK**.

Edit Advanced vSphere Distributed Switch Settings

You can change advanced vSphere distributed switch settings such as Cisco Discovery Protocol and the maximum MTU for the vSphere distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select **Advanced** to edit the following vSphere distributed switch settings.

Option	Description
Maximum MTU	Maximum MTU size for the vSphere distributed switch.
Discovery Protocol Status	Choose the status for discovery protocol on the vSphere distributed switch. ■ **Enabled**. Enabled discovery protocol for the vSphere distributed switch. 1 Select **Cisco Discovery Protocol** or **Link Layer Discovery Protocol** from the **Type** drop-down menu. 2 Set **Operation** to **Listen**, **Advertise**, or **Both**. ■ **Disabled**.
Admin Contact Info	Enter the **Name** and **Other Details** for the vSphere distributed switch administrator.

4 Click **OK**.

View Network Adapter Information for a vSphere Distributed Switch

View physical network adapters and uplink assignments for a vSphere distributed switch from the networking inventory view of the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Network Adapters** tab, you can view network adapter and uplink assignments for associated hosts.

This tab is read-only. Distributed switch network adapters must be configured at the host level.

4 Click **OK**.

Upgrade a vSphere Distributed Switch to a Newer Version

A vSphere distributed switch version 4.0 or newer can be upgraded to a later version, enabling the distributed switch to take advantage of features that are only available in the later version.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Summary** tab, next to **Version**, select **Upgrade**.

The upgrade wizard details the features available to the upgraded distributed switch that are not available to the earlier version.

4 Select the vSphere Distributed Switch version to upgrade to.

Option	Description
vSphere Distributed Switch Version: 4.1.0	Compatible with ESX/ESXi version 4.1 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 5.0.0	Compatible with ESXi version 5.0 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 5.1.0	Compatible with ESXi version 5.1 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 5.5.0	Compatible with ESXi version 5.5 and later. Features released with later vSphere distributed switch versions are not supported.
vSphere Distributed Switch Version: 6.0.0	Compatible with ESXi version 6.0 and later.

5 Click **Next**.

The upgrade wizard lists the hosts associated with this vSphere distributed switch and whether or not they are compatible with the upgraded vSphere distributed switch version. You can proceed with the upgrade only if all hosts are compatible with the new vSphere distributed switch version.

Next to each incompatible host is the reason for the incompatibility.

6 Click **Next**.

7 Verify that the upgrade information listed is correct and click **Finish**.

Distributed Port Groups

A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

Add a Distributed Port Group

Add a distributed port group to a vSphere distributed switch to create a distributed switch network for your virtual machines.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane and select **New Port Group**.

3 Enter a **Name** and the **Number of Ports** for your new distributed port group.

4 Select a VLAN Type.

Option	Description
None	Do not use VLAN.
VLAN	In the **VLAN ID** field, enter a number between 1 and 4094.
VLAN Trunking	Enter a VLAN trunk range.
Private VLAN	Select a private VLAN entry. If you did not create any private VLANs, this menu is empty.

5 Click **Next**.

6 Click **Finish**.

Edit General Distributed Port Group Settings

You can edit general distributed port group settings such as the distributed port group name and port group type.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **General** to edit the following distributed port group settings.

Option	Action
Name	Type the name for the distributed port group.
Description	Type a brief description of the distributed port group.
Number of Ports	Type the number of ports on the distributed port group.
Port binding	Choose when ports are assigned to virtual machines connected to this distributed port group. ■ Select **Static binding** to assign a port to a virtual machine when the virtual machine connects to the distributed port group. This option is not available when the vSphere Client is connected directly to ESXi. ■ Select **Dynamic binding** to assign a port to a virtual machine the first time the virtual machine powers on after it is connected to the distributed port group. Dynamic binding is deprecated in ESXi 5.x. ■ Select **Ephemeral** for no port binding. This option is not available when the vSphere Client is connected directly to ESXi.

4 Click **OK**.

Edit Advanced Distributed Port Group Settings

You can edit advanced distributed port group settings, such as override settings and reset at disconnect.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Advanced** to edit the distributed port group properties.

Option	Description
Allow override of port policies	Select this option to allow distributed port group policies to be overridden on a per-port level. Click **Edit Override Settings** to select which policies can be overridden at the port level.
Edit Override Settings	Select which policies can be overridden at the port level.
Configure reset at disconnect	When a distributed port is disconnected from a virtual machine, the configuration of the distributed port is reset to the distributed port group setting. Any per-port overrides are discarded.

4 Click **OK**.

Monitor Distributed Port State

vSphere can monitor distributed ports and provide information on the current state of each port and the port's runtime statistics.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, click **Start Monitoring Port State**.

The table on the Ports tab for the distributed switch now displays runtime statistics for each distributed port, including broadcast, multicast, and unicast ingress and egress traffic and packets.

The **State** column displays the current state for each distributed port.

Table 20-2. Distributed Port States

State	Description
Link Up	The link for this distributed port is up.
Link Down	The link for this distributed port is down.
Blocked	This distributed port is blocked.
--	The state of this distributed port is currently unavailable.

Configure Distributed Port Settings

You can change general distributed port settings such as the port name and description.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **General**.

5 Modify the port name and description.

6 Click **OK**.

Private VLANs

Private VLANs are used to solve VLAN ID limitations and waste of IP addresses for certain network setups.

A private VLAN is identified by its primary VLAN ID. A primary VLAN ID can have multiple secondary VLAN IDs associated with it. Primary VLANs are **Promiscuous**, so that ports on a private VLAN can communicate with ports configured as the primary VLAN. Ports on a secondary VLAN can be either **Isolated**, communicating only with promiscuous ports, or **Community**, communicating with both promiscuous ports and other ports on the same secondary VLAN.

To use private VLANs between a host and the rest of the physical network, the physical switch connected to the host needs to be private VLAN-capable and configured with the VLAN IDs being used by ESXi for the private VLAN functionality. For physical switches using dynamic MAC+VLAN ID based learning, all corresponding private VLAN IDs must be first entered into the switch's VLAN database.

Create a Private VLAN

You can create a private VLAN for use on a vSphere distributed switch and its associated distributed ports.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select the **Private VLAN** tab.

4 Under Primary Private VLAN ID, click **[Enter a Private VLAN ID here]**, and enter the number of the primary private VLAN.

5 Click anywhere in the dialog box, and then select the primary private VLAN that you just added.

   The primary private VLAN you added appears under Secondary Private VLAN ID.

6 For each new secondary private VLAN, click **[Enter a Private VLAN ID here]** under Secondary Private VLAN ID, and enter the number of the secondary private VLAN.

7 Click anywhere in the dialog box, select the secondary private VLAN that you just added, and select either **Isolated** or **Community** for the port type.

8 Click **OK**.

Remove a Primary Private VLAN

Remove unused primary private VLANs from the networking inventory view of the vSphere Client.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.
- Before removing a private VLAN, be sure that no port groups are configured to use it.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select the **Private VLAN** tab.

4 Select the primary private VLAN to remove.

5 Click **Remove** under Primary Private VLAN ID, and click **OK**.

Removing a primary private VLAN also removes all associated secondary private VLANs.

Remove a Secondary Private VLAN

Remove unused secondary private VLANs from the networking inventory view of the vSphere Client.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that you have sufficient permissions to edit a distributed switch.
- Before removing a private VLAN, be sure that no port groups are configured to use it.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Select the **Private VLAN** tab.

4 Select a primary private VLAN to display its associated secondary private VLANs.

5 Select the secondary private VLAN to remove.

6 Click **Remove** under Secondary Private VLAN ID, and click **OK**.

Managing Physical Adapters

For each host associated with a vSphere distributed switch, you must assign physical network adapters, or uplinks, to the vSphere distributed switch. You can assign one uplink on each host per uplink port on the vSphere distributed switch.

Add an Uplink to a vSphere Distributed Switch

For each host associated with a vSphere distributed switch, you must assign at least one physical network adapter, or uplink, to the vSphere distributed switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select the **vSphere Distributed Switch** view.

4 Click **Manage Physical Adapters**.

5 Click **Click to Add NIC** for the uplink port to add an uplink to.

6 Select the physical adapter to add.

   If you select an adapter that is attached to another switch, it will be removed from that switch and reassigned to this vSphere distributed switch.

7 Click **OK**.

Remove an Uplink from a vSphere Distributed Switch

You can remove an uplink, or physical network adapter, from a vSphere distributed switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select the **vSphere Distributed Switch** view.

4 Click **Manage Physical Adapters**.

5 Click **Remove** to remove the uplink from the vSphere distributed switch.

6 Click **OK**.

Remove NICs from Active Virtual Machines

When you remove NICs from active virtual machines, you may still see the NICs you removed reported in the vSphere Client.

Remove NICs from an active virtual machine without a guest operating system installed

You cannot remove NICs from an active virtual machine if the virtual machine has no operating system installed.

The vSphere Client might report that the NIC has been removed, but you will continue to see it attached to the virtual machine.

Remove NICs from an active virtual machine with a guest operating system installed

You can remove a NIC from an active virtual machine, but it might not be reported to the vSphere Client for some time. If you open **Edit Settings** for the virtual machine, you might still see the NIC that you removed listed, even when the task is complete. The **Edit Settings** dialog box for the virtual machine does not immediately display the removed NIC.

You may also still see the NIC attached to the virtual machine if the guest operating system of the virtual machine does not support hot-removal of NICs.

Managing Virtual Network Adapters

Virtual network adapters handle host network services over a vSphere distributed switch.

You can configure VMkernel virtual adapters for a host through an associated vSphere distributed switch either by creating new virtual adapters or migrating existing virtual adapters.

Create a VMkernel Network Adapter on a vSphere Distributed Switch

Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Select the vSphere Distributed Switch view.

4 Click **Manage Virtual Adapters**.

5 Click **Add**.

6 Select **New virtual adapter**, and click **Next**.

7 Select **VMkernel** and click **Next**.

8 Choose a distributed port or distributed port group connection for the virtual adapter.

Option	Description
Select a port group	Choose the distributed port group for the virtual adapter to connect to from the drop-down menu.
Select port	Type the port ID of the distributed port for the virtual network adapter to connect to.

9 Select **Use this virtual adapter for vMotion** to enable this port group to advertise itself to another ESXi host as the network connection where vMotion traffic is sent.

   You can enable this property for only one vMotion and IP storage port group for each host. If this property is not enabled for any port group, migration with vMotion to this host is not possible.

10 Choose whether to **Use this virtual adapter for Fault Tolerance logging**.

11 Choose whether to **Use this virtual adapter for management traffic**, and click **Next**.

12 Under IP Settings, specify the IP address and subnet mask.

   IPv6 cannot be used with a dependent hardware iSCSI adapter.

13 Click **Edit** to set the VMkernel default gateway for VMkernel services, such as vMotion, NAS, and iSCSI.

14 On the **DNS Configuration** tab, the name of the host is entered by default. The DNS server addresses and domain that were specified during installation are also preselected.

15 On the **Routing** tab, enter gateway information for the VMkernel. A gateway is needed for connectivity to machines not on the same IP subnet as the VMkernel.

   Static IP settings is the default. Do not use routing with software iSCSI Multipathing configurations or dependent hardware iSCSI adapters.

16 Click **OK**, and then click **Next**.

17 Click **Finish**.

Migrate an Existing Virtual Adapter to a vSphere Distributed Switch

You can migrate an existing virtual adapter from a vSphere standard switch to a vSphere distributed switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Select the vSphere Distributed Switch view.

4 Click **Manage Virtual Adapters**.

5 Click **Add**.

6 Select **Migrate existing virtual network adapters** and click **Next**.

7 Select one or more virtual network adapters to migrate.

8 For each selected adapter, choose a port group from the **Select a port group** drop-down menu.

9 Click **Next**.

10 Click **Finish**.

Migrate a Virtual Adapter to a vSphere Standard Switch

You can migrate an existing virtual adapter from a vSphere distributed switch to a vSphere standard switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Select the vSphere Distributed Switch view.

4 Click **Manage Virtual Adapters**.

5 Select the virtual adapter to migrate, and click **Migrate**.

6 Select the standard switch to migrate the adapter to and click **Next**.

7 Enter a **Network Label** and optionally a **VLAN ID** for the virtual adapter, and click **Next**.

8 Click **Finish** to migrate the virtual adapter and complete the wizard.

Edit VMkernel Configuration on a vSphere Distributed Switch

You can edit a VMkernel virtual network adapter on a vSphere distributed switch to change the IP settings, such as IP address, subnet mask, default gateway, and DNS configuration. You can also select whether the virtual adapter is used for vMotion or fault tolerance logging.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Select the vSphere Distributed Switch view.

4 Click **Manage Virtual Adapters**.

5 Select the VMkernel adapter to modify and click **Edit**.

6 Under Network Connection, select **vSphere Distributed Switch** and **Port Group** or **Port** to add this virtual adapter to.

7 Select **Use this virtual adapter for vMotion** to enable this port group to advertise itself to another host as the network connection that vMotion traffic should be sent through.

   You can enable this property for only one vMotion and IP storage port group for each host. If this property is not enabled for any port group, migration with vMotion to this host is not possible.

8 (Optional) Select **Use this virtual adapter for fault tolerance logging**.

9 (Optional) Select **Use this virtual adapter for management traffic**.

10 Under IP Settings, specify the **IP Address** and **Subnet Mask**, or select **Obtain IP settings automatically** .

11 Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI.

   On the **DNS Configuration** tab, the name of the host appears in the name field by default. The DNS server addresses that were specified during installation are also preselected, as is the domain.

   On the **Routing** tab, a gateway is needed for connectivity to machines not on the same IP subnet as the VMkernel.

   Static IP settings is the default.

12 Use the up and down arrows to set the MTU for the VMkernel adapter.

13 Click **OK**.

View VMkernel Routing Information on a vSphere Distributed Switch

You can view IP and IPv6 routing information, such as network, prefix, and gateway, for a VMkernel network adapter on a vSphere distributed switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 In the vSphere Distributed Switch view, click **Manage Virtual Adapters**.

4 Select the VMkernel adapter to view, and click **View Routing Table** under IP Settings or IPv6 Settings.

A routing table that includes network, prefix, and gateway information for the selected VMkernel adapter appears.

Remove a Virtual Adapter

Remove a virtual network adapter from a vSphere distributed switch in the Manage Virtual Adapters dialog box.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere Distributed Switch view.

4 Click **Manage Virtual Adapters**.

5 Select the virtual adapter to remove and click **Remove**.

   A dialog box appears with the message, `Are you sure you want to remove` *`adapter name`*`?`

6 Click **Yes**.

Configuring Virtual Machine Networking on a vSphere Distributed Switch

Connect virtual machines to a vSphere distributed switch either by configuring an individual virtual machine NIC or migrating groups of virtual machines from the vSphere distributed switch itself.

Connect virtual machines to vSphere distributed switches by connecting their associated virtual network adapters to distributed port groups. You can do this either for an individual virtual machine by modifying the virtual machine's network adapter configuration, or for a group of virtual machines by migrating virtual machines from an existing virtual network to a vSphere distributed switch.

Migrate Virtual Machines to Or from a vSphere Distributed Switch

In addition to connecting virtual machines to a distributed switch at the individual virtual machine level, you can migrate a group of virtual machines between a vSphere distributed switch network and a vSphere standard switch network.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the datacenter and select **Migrate Virtual Machine Networking**.

   The Migrate Virtual Machine Networking wizard appears.

3 Select a **Source Network** to migrate adapters from.

Option	Description
Include all virtual machine network adapters that are connected to the following network (Filter by Network)	Migrates virtual machine network adapters from a particular network. Select the source network from the **Network** drop-down menu.
Include all virtual machine network adapters that are connected to the following network (Filter by VDS)	Migrates virtual machine network adapters from a network on a particular vSphere distributed switch. To migrate from a network, select **Switch** and **Network** from the drop-down menus.
Include all virtual machine network adapters that are not connected to any network	Migrates virtual machine network adapters that are not connected to any network.

4 Select a **Destination Network** to migrate adapters to.

Option	Description
Filter by Network	Migrates virtual machine network adapters to a particular network. Select the destination network from the **Network** drop-down menu.
Filter by VDS	Migrates virtual machine network adapters to a network on a particular vSphere Distritubed Switch. To migrate to a network, select **Switch** and **Network** from the drop-down menus.

5 Click **Next**.

6 (Optional) Highlight a virtual machine or adapter to view their details.

7 Select the virtual machines and adapters to migrate to the destination network and click **Next**.

8 Verify that the source network, destination network, and number of virtual machines to migrate are correct and click **OK**.

Connect an Individual Virtual Machine to a Distributed Port Group

Connect an individual virtual machine to a vSphere distributed switch by modifying the virtual machine's NIC configuration.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the virtual machine from the inventory panel.

2 On the **Summary** tab, click **Edit Settings**.

3 On the **Hardware** tab, select the virtual network adapter.

4 Select the distributed port group to migrate to from the **Network Label** drop-down menu, and click **OK**.

Managing Network Resources 21

vSphere provides several different methods to help you manage your network resources.

This chapter includes the following topics:

- "vSphere Network I/O Control," on page 247
- "TCP Segmentation Offload and Jumbo Frames," on page 250
- "DirectPath I/O," on page 252
- "Single Root I/O Virtualization (SR-IOV)," on page 254

vSphere Network I/O Control

Use vSphere Network I/O Control to allocate network bandwidth to business-critical applications and to resolve situations where several types of traffic compete for common resources.

Enable Network I/O Control on a vSphere Distributed Switch

Enable network resource management to use network resource pools to prioritize network traffic by type.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Verify that your datacenter has at least one vSphere distributed switch version 4.1.0 or later.

Procedure

1. Log in to the vSphere Client and select the **Networking** inventory view.
2. Select the vSphere distributed switch in the inventory pane.
3. On the **Resource Allocation** tab, click **Properties**.
4. Select **Enable Network I/O Control on this vSphere ditributed switch**, and click **OK**.

Create a Network Resource Pool

Create user-defined network resource pools for customized network resource management.

User-defined network resource pools are available only on vSphere distributed switches version 5.0.0 or later.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Resource Allocation**tab, click **New Network Resource Pool**.

4 Type a **Name** for the network resource pool.

5 (Optional) Type a **Description** for the network resource pool.

6 Select the **Physical adapter shares** for the network resource pool.

Option	Description
Custom	Type a specific number of shares, from 1 to 100, for this network resource pool.
High	Sets the shares for this resource pool to 100.
Normal	Sets the shares for this resource pool to 50.
Low	Sets the shares for this resource pool to 25.

7 Set the **Host limit** for the network resource pool in megabits per second or select **Unlimited**.

8 (Optional) Select the **QoS priority tag** for the network resource pool.

9 Click **OK**.

The new resource pool appears on the **Resource Allocation** tab under User-defined network resource pools.

What to do next

Add one or more distributed port groups to the network resource pool.

Add or Remove Distributed Port Groups from a Network Resource Pool

Add a distributed port group to a user-defined network resource pool to include in the network resource pool all virtual machine network traffic from that distributed port group.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Create one or more network resource pools on the vSphere distributed switch.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Resource Allocation** tab, click **Manage Port Groups**.

4 (Optional) Select the user-defined network resource pool to associate with a single distributed port group from the Network resource pool drop-down menu or select **None** to remove that distributed port group from a user-defined resource pool.

5 (Optional) Select the user-defined network resource pool to associate with multiple distributed port groups.

   a Hold Ctrl to select multiple distributed port groups to modify, and click **Assign multiple**.

   b Select the user-defined network resource pool to associate with the distributed port groups from the Network Resource Pool drop-down menu, or select **None** to remove the distributed port groups from all user-defined resource pools.

6 Click **OK**.

Edit Network Resource Pool Settings

You can change network resource pool settings such as allocated shares and limits for each network resource pool to change the priority network traffic for that network resource pool is given.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Resource Allocation** tab, right-click the network resource pool to edit, and select **Edit Settings**.

4 Select the **Physical adapter shares** for the network resource pool.

Option	Description
Custom	Enter a specific number of shares, from 1 to 100, for this network resource pool.
High	Sets the shares for this resource pool to 100.
Normal	Sets the shares for this resource pool to 50.
Low	Sets the shares for this resource pool to 25.

5 Set the **Host limit** for the network resource pool in megabits per second or select **Unlimited**.

6 (Optional) Select the **QoS priority tag** from the drop-down menu.

The QoS priority tag specifies an IEEE 802.1p tag, allowing quality of service at the media access control level

7 Click **OK**.

Delete a Network Resource Pool

You can delete user-defined network resource pools that are no longer in use.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Remove all distributed port groups from the network resource pool.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Resource Allocation** tab, right-click the user-defined network resource pool to delete, and select **Remove**.

4 Click **Yes**.

TCP Segmentation Offload and Jumbo Frames

Using TCP Segmentation Offload (TSO) in a VMkernel network adapter and virtual machines, and jumbo frames on a vSphere distributed switch or vSphere standard switch, improves the network performance in virtual machines and infrastructure workloads.

Enable TSO Support for a Virtual Machine

You can enable TSO support on a virtual machine by using an enhanced vmxnet adapter for that virtual machine.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the virtual machine from the inventory panel.

2 Click the **Summary** tab, and click **Edit Settings**.

3 Select the network adapter from the Hardware list.

4 Record the network settings and MAC address that the network adapter is using.

5 Click **Remove** to remove the network adapter from the virtual machine.

6 Click **Add**.

7 Select **Ethernet Adapter** and click **Next**.

8 In the Adapter Type group, select **Enhanced vmxnet**.

9 Select the network setting and MAC address that the old network adapter was using and click **Next**.

10 Click **Finish** and then click **OK**.

11 If the virtual machine is not set to upgrade VMware Tools at each power on, you must upgrade VMware Tools manually.

TSO is enabled on a VMkernel interface. If TSO becomes disabled for a particular VMkernel interface, the only way to enable TSO is to delete that VMkernel interface and recreate it with TSO enabled.

Enable Jumbo Frames for a VMkernel Interface on a vSphere Standard Switch

Jumbo frames reduce the CPU load caused by transferring data. Enable jumbo frames on a VMkernel network interface by changing the maximum transmission units (MTU) of the VMkernel interface.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Click **Properties** for the vSphere standard switch associated with the VMkernel to modify.

4 On the **Ports** tab, select the VMkernel interface and click **Edit**.

5 Set the **MTU** to 9000, and click **OK**.

Enable Jumbo Frames on a vSphere Distributed Switch

Enable a vSphere distributed switch for jumbo frames by changing the MTU size for that distributed switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Properties** tab, select **Advanced**.

4 Set the **Maximum MTU** to the largest MTU size among all the virtual network adapters connected to the vSphere distributed switch, and click **OK**.

Enable Jumbo Frame Support on a Virtual Machine

Enabling jumbo frame support on a virtual machine requires an enhanced vmxnet adapter for that virtual machine.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the virtual machine from the inventory panel.

2 Click the **Summary** tab, and click **Edit Settings**.

3 Select the network adapter from the Hardware list.

4 Record the network settings and MAC address that the network adapter is using.

5 Click **Remove** to remove the network adapter from the virtual machine.

6 Click **Add**.

7 Select **Ethernet Adapter** and click **Next**.

8 In the Adapter Type group, select **Enhanced vmxnet**.

9 Select the network that the old network adapter was using and click **Next**.

10 Click **Finish**.

11 Select the new network adapter from the Hardware list.

12 Under MAC Address, select **Manual**, and enter the MAC address that the old network adapter was using.

13 Click **OK**.

14 Check that the Enhanced vmxnet adapter is connected to a standard switch or distributed switch with jumbo frames enabled.

15 Inside the guest operating system, configure the network adapter to allow jumbo frames.

   See your guest operating system's documentation for details.

16 Configure all physical switches and any physical or virtual machines to which this virtual machine connects to support jumbo frames.

DirectPath I/O

DirectPath I/O allows virtual machine access to physical PCI functions on platforms with an I/O Memory Management Unit.

The following features are unavailable for virtual machines configured with DirectPath:

- Hot adding and removing of virtual devices
- Suspend and resume
- Record and replay
- Fault tolerance
- High availability
- DRS (limited availability. The virtual machine can be part of a cluster, but cannot migrate across hosts)
- Snapshots

The following features are only available for virtual machines configured with DirectPath I/O on Cisco Unified Computing Systems (UCS) through Cisco Virtual Machine Fabric Extender (VM-FEX) distributed switches.

- vMotion
- Hot adding and removing of virtual devices
- Suspend and resume
- High availability
- DRS
- Snapshots

See Cisco VM-FEX documentation for details on supported switches and switch configuration information.

Configure Passthrough Devices on a Host

You can configure passthrough networking devices on a host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a host from the inventory panel of the vSphere Client.

2 On the **Configuration** tab, click **Advanced Settings**.

   The Passthrough Configuration page appears, listing all available passthrough devices. A green icon indicates that a device is enabled and active. An orange icon indicates that the state of the device has changed and the host must be rebooted before the device can be used.

3 Click **Edit**.

4 Select the devices to be used for passthrough and click **OK**.

Configure a PCI Device on a Virtual Machine

You can configure a passthrough PCI device on a virtual machine.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a virtual machine from the inventory panel of the vSphere Client.

2 From the **Inventory** menu, select **Virtual Machine > Edit Settings**.

3 On the **Hardware** tab, click **Add**.

4 Select **PCI Device** and click **Next**.

5 Select the passthrough device to use, and click **Next**.

6 Click **Finish**.

Adding a DirectPath device to a virtual machine sets memory reservation to the memory size of the virtual machine.

Enable DirectPath I/O with vMotion on a Virtual Machine

You can enable DirectPath I/O with vMotion for virtual machines in a datacenter on a Cisco UCS system that has at least one supported Cisco UCS Virtual Machine Fabric Extender (VM-FEX) distributed switch.

Prerequisites

- Enable high performance network I/O on at least one Cisco UCS port profile on a supported Cisco VM-FEX distributed switch. For supported switches and switch configuration, see Cisco's documentation at http://www.cisco.com/go/unifiedcomputing/b-series-doc.

  Launch the vSphere Client and log in to a vCenter Server system.

- Power off the virtual machine.

Procedure

1 Log in to the vSphere Client and select the VMs and Templates inventory view.

2 Right-click the virtual machine to modify and click **Edit Settings**.

3 On the **Resources** tab, select **Memory**.

4 Select **Unlimited**.

5 On the **Hardware** tab, select the network adapter to configure as a passthrough device.

6 Select a port profile with high performance enabled from the network label drop-down menu, and click **OK**.

7 Power on the virtual machine.

  After the virtual machine is powered on, DirectPath I/O appears as Active on the **Hardware** tab of the virtual machine properties dialog box.

Single Root I/O Virtualization (SR-IOV)

vSphere 5.1 and later releases support Single Root I/O Virtualization (SR-IOV). You can use SR-IOV for networking of virtual machines that are latency sensitive or require more CPU resources.

Overview of SR-IOV

SR-IOV is a specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear as multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices. PFs are full PCIe functions that are capable of configuring and managing the SR-IOV functionality. It is possible to configure or control PCIe devices using PFs, and the PF has full ability to move data in and out of the device. VFs are lightweight PCIe functions that support data flowing but have a restricted set of configuration resources.

The number of virtual functions provided to the hypervisor or the guest operating system depends on the device. SR-IOV enabled PCIe devices require appropriate BIOS and hardware support, as well as SR-IOV support in the guest operating system driver or hypervisor instance. See the *vSphere Networking* publication for more information.

Using SR-IOV in vSphere

In vSphere, a virtual machine can use an SR-IOV virtual function for networking. The virtual machine and the physical adapter exchange data directly without using the VMkernel as an intermediary. Bypassing the VMkernel for networking reduces latency and improves CPU efficiency.

In vSphere 5.5 and later, though a virtual switch (standard switch or distributed switch) does not handle the network traffic of an SR-IOV enabled virtual machine connected to the switch, you can control the assigned virtual functions by using switch configuration policies at port group or port level.

Configure SR-IOV in a Host Profile

Before you can connect a virtual machine to a virtual function, you must configure the virtual functions of the physical NIC on your host by using a host profile.

You can also enable SR-IOV virtual functions on the host by using the `esxcli system module parameters set` vCLI command on the NIC driver parameter for virtual functions in accordance with the driver documentation. For more information about using vCLI commands, see *vSphere Command-Line Interface Documentation*.

Prerequisites

- Verify that the configuration of your environment supports SR-IOV. See SR-IOV Support.
- Create a host profile using the SR-IOV capable host as a reference. For more information about host profiles, see the *vSphere Host Profiles* documentation.

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client, click **Home** and select the **Host Profiles** main view.
2. Select the host profile from the list and click **Edit Profile**.
3. Expand `Kernel Module Configuration > Kernel Module` and select the kernel module for the physical function driver.

4 Expand **Kernel Module Parameter** and select the parameter of the physical function driver for creating virtual functions.

   For example, the parameter for the physical function driver of an Intel physical NIC is **max_vfs**.

5 Click **Edit**.

6 In the **Value** text box, type a comma-separated list of valid virtual function numbers.

   Each list entry is the number of virtual functions that you want to configure for each physical function. A value of 0 means SR-IOV will not be enabled for that physical function.

   For example, if you have a dual port, set the value to

   `x,y`

   where `x` or `y` is the number of virtual functions you want to enable for a single port.

   If the target number of virtual functions on a single host is 30, you might have two dual port cards set to `0,10,10,10`.

   NOTE The number of virtual functions supported and available for configuration depends on your system configuration.

7 Click **OK**.

8 Remediate the modified host profile to the target host.

After the virtual functions become enabled on the host, the physical NIC no longer shows up as a host network adapter in the **Network Adapters** list within the **Configuration** tab for the host. It appears in the **Advanced Settings** list for the host.

What to do next

Associate a virtual function with a virtual machine as a PCI device for networking through Direct Path I/O.

Assign a Virtual Function to a Virtual Machine

To ensure that a virtual machine and a physical NIC can exchange data, you must associate a virtual machine with one or more virtual functions.

After you enable the virtual functions on the host, each of them becomes available as a PCI device.

Launch the vSphere Client and log in to a vCenter Server system.

Prerequisites

- Verify that the configuration of your environment supports SR-IOV. See SR-IOV Support.
- Verify that the virtual functions exist on the host.
- Verify that the passthrough networking device for the virtual function is active on the host.

Procedure

1 Select a virtual machine from the inventory panel of the vSphere Client.

2 Power off the virtual machine.

3 From the **Inventory** menu, select **Virtual Machine > Edit Settings**.

4 On the **Resources** tab, select **Memory**.

5 Select **Unlimited**.

6 On the **Hardware** tab, click **Add**.

7 Select **PCI Device** and click **Next**.

8 From the drop-down menu select the virtual function.

9 Click **Finish**.

10 Power on the virtual machine.

Adding a virtual function as a PCI device to a virtual machine sets memory reservation to the memory size of the virtual machine.

Configure the Passthrough Device for a Virtual Function

After you configure a virtual machine with a virtual function as a PCI device, you can configure the virtual function with a static MAC address and a default VLAN with the help of the vSphere Client.

In the virtual machine configuration `.vmx` file, you can assign a static MAC address and a default VLAN to the virtual function.

Prerequisites

Verify that the virtual function is assigned to the virtual machine as a PCI device.

Procedure

1 Select a virtual machine from the inventory panel of the vSphere Client.

2 Power off the virtual machine.

3 From the **Inventory** menu, select **Virtual Machine > Edit Settings**.

4 Click the **Options** tab and under **Advanced** select **General**.

5 Click **Configuration**.

6 To assign a static MAC address, add or edit the following parameters.

Parameter	Value
`pciPassthruX.MACAddressType`	static
`pciPassthruX.MACAddress`	*MAC_address_of_the_virtual_function*

`X` next to `pciPassthru` stands for the sequence number of the PCI device in the virtual machine. For example, 0 in `pciPassthru0` represents the settings of the PCI device added first to the virtual machine.

7 To assign a default VLAN, add or edit the `pciPassthruX.defaultVlan` parameter according to the following value guidelines. `X` next to `pciPassthru` stands for the sequence number of the PCI device in the virtual machine.

Option	Description
0	Allow no VLAN and do NOT allow guest VLAN tagging. In this way, administratively disallow guest VLAN tagging.
1-4095	Allow tagged only and do NOT allow guest VLAN tagging.
No entry	Allow untagged only and allow guest VLAN tagging.

8 Click **OK**.

9 Power on the virtual machine.

Networking Policies 22

Policies set at the standard switch or distributed port group level apply to all of the port groups on the standard switch or to ports in the distributed port group. The exceptions are the configuration options that are overridden at the standard port group or distributed port level.

This chapter includes the following topics:

- "Applying Networking Policies on a vSphere Standard or Distributed Switch," on page 257
- "Teaming and Failover Policy," on page 259
- "VLAN Policy," on page 267
- "Security Policy," on page 269
- "Traffic Shaping Policy," on page 273
- "Resource Allocation Policy," on page 277
- "Monitoring Policy," on page 278
- "Port Blocking Policies," on page 279
- "Manage Policies for Multiple Port Groups on a vSphere Distributed Switch," on page 279

Applying Networking Policies on a vSphere Standard or Distributed Switch

You apply networking policies differently on vSphere Standard Switches and vSphere Distributed Switches. Not all policies that are available for a vSphere Distributed Switch are also available for a vSphere Standard Switch.

Table 22-1. Virtual Switch Objects Where Policies Apply

Virtual Switch	Virtual Switch Object	Description
vSphere Standard Switch	Entire switch	When you apply policies on the entire standard switch, the policies are propagated to all standard port groups on the switch.
	Standard port group	You can apply different policies on individual port groups by overriding the policies that are inherited from the switch.
vSphere Distributed Switch	Distributed port group	When you apply policies on a distributed port group, the policies are propagated to all ports in the group.
	Distributed port	You can apply different policies on individual distributed ports by overriding the policies that are inherited from the distributed port group.

Table 22-1. Virtual Switch Objects Where Policies Apply (Continued)

Virtual Switch	Virtual Switch Object	Description
	Uplink port group	You can apply policies at uplink port group level, and the are policies are propagated to all ports in the group.
	Uplink port	You can apply different policies on individual uplink ports by overriding the policies that are inherited from the uplink port group.

Table 22-2. Policies Available for a vSphere Standard Switch and vSphere Distributed Switch

Policy	Standard Switch	Distributed Switch	Description
Teaming and failover	Yes	Yes	Lets you configure the physical NICs that handle the network traffic for a standard switch, standard port group, distributed port group, or distributed port. You arrange the physical NICs in a failover order and apply different load balancing policies over them.
Security	Yes	Yes	Provides protection of traffic against MAC address impersonation and unwanted port scanning. The networking security policy is implemented in Layer 2 of the networking protocol stack.
Traffic shaping	Yes	Yes	Lets you restrict the network bandwidth that is available to ports, but also to allow bursts of traffic to flow through at higher speeds. ESXi shapes outbound network traffic on standard switches and inbound and outbound traffic on distributed switches.
VLAN	Yes	Yes	Lets you configure the VLAN tagging for a standard or distributed switch. You can configure External Switch Tagging(EST), Virtual Switch Tagging (VST), and Virtual Guest Tagging (VGT).
Monitoring	No	Yes	Enables and disables NetFlow monitoring on a distributed port or port group.
Traffic filtering and marking	No	Yes	Lest you protect the virtual network from unwanted traffic and security attacks or apply a QoS tag to a certain traffic type.
Resources allocation	No	Yes	Lets you associate a distributed port or port group with a user-defined network resource pool. In this way, you can better control the bandwidth that is available to the port or port group. You can use the resource allocation policy with vSphere Network I/O Control version 2 and 3.
Port blocking	No	Yes	Lets you selectively block ports from sending and receiving data.

Teaming and Failover Policy

NIC teaming lets you increase the network capacity of a virtual switch by including two or more physical NICs in a team. To determine how the traffic is rerouted in case of adapter failure, you include physical NICs in a failover order. To determine how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing algorithms depending on the needs and capabilities of your environment.

NIC Teaming Policy

You can use NIC teaming to connect a virtual switch to multiple physical NICs on a host to increase the network bandwidth of the switch and to provide redundancy. A NIC team can distribute the traffic between its members and provide passive failover in case of adapter failure or network outage. You set NIC teaming policies at virtual switch or port group level for a vSphere Standard Switch and at a port group or port level for a vSphere Distributed Switch.

NOTE All ports on the physical switch in the same team must be in the same Layer 2 broadcast domain.

Load Balancing Policy

The Load Balancing policy determines how network traffic is distributed between the network adapters in a NIC team. vSphere virtual switches load balance only the outgoing traffic. Incoming traffic is controlled by the load balancing policy on the physical switch.

For more information about each load balancing algorithm, see the *vSphere Networking* publication.

Network Failure Detection Policy

You can specify one of the following methods that a virtual switch uses for failover detection.

Link status only

Relies only on the link status that the network adapter provides. Detects failures, such as removed cables and physical switch power failures. However, link status does not detect the following configuration errors:

- Physical switch port that is blocked by spanning tree or is misconfigured to the wrong VLAN .
- Pulled cable that connects a physical switch to another networking devices, for example, an upstream switch .

Beacon probing

Sends out and listens for Ethernet broadcast frames, or beacon probes, that physical NICs send to detect link failure in all physical NICs in a team. ESXi hosts send beacon packets every second. Beacon probing is most useful to detect failures in the closest physical switch to the ESXi host, where the failure does not cause a link-down event for the host.

Use beacon probing with three or more NICs in a team because ESXi can detect failures of a single adapter. If only two NICs are assigned and one of them loses connectivity, the switch cannot determine which NIC needs to be taken out of service because both do not receive beacons and as a result all packets sent to both uplinks. Using at least three NICs in such a team allows for n-2 failures where *n* is the number of NICs in the team before reaching an ambiguous situation.

Failback Policy

By default, a failback policy is enabled on a NIC team. If a failed physical NIC returns online, the virtual switch sets the NIC back to active by replacing the standby NIC that took over its slot.

If the physical NIC that stands first in the failover order experiences intermittent failures, the failback policy might lead to frequent changes in the NIC that is used. The physical switch sees frequent changes in MAC addresses, and the physical switch port might not accept traffic immediately when an adapter becomes online. To minimize such delays, you might consider changing the following settings on the physical switch:

- Disable Spanning Tree Protocol (STP) on physical NICs that are connected to ESXi hosts .
- For Cisco based networks, enable PortFast mode for access interfaces or PortfFast trunk mode for trunk interfaces. This might save about 30 seconds during the initialization of the physical switch port.
- Disable the trunking negotiation.

Notify Switches Policy

By using the notify switches policy, you can determine how the ESXi host communicates failover events. When a physical NIC connects to the virtual switch or when traffic is rerouted to a different physical NIC in the team, the virtual switch sends notifications over the network to update the lookup tables on physical switches. Notifying the physical switch offers lowest latency when a failover or a migration with vSphere vMotion occurs.

Edit Failover and Load Balancing Policy for a vSphere Standard Switch

Use Load Balancing and Failover policies to determine how network traffic is distributed between adapters and how to reroute traffic in the event of an adapter failure.

The Failover and Load Balancing policies include the following parameters:

- Load Balancing policy: The Load Balancing policy determines how outgoing traffic is distributed among the network adapters assigned to a standard switch. Incoming traffic is controlled by the Load Balancing policy on the physical switch.
- Failover Detection: Link Status/Beacon Probing
- Network Adapter Order (Active/Standby)

In some cases, you might lose standard switch connectivity when a failover or failback event occurs. This causes the MAC addresses used by virtual machines associated with that standard switch to appear on a different switch port than they previously did. To avoid this problem, put your physical switch in portfast or portfast trunk mode.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. Log in to the vSphere Client and select a host in the inventory pane.
2. Click the **Configuration** tab and click **Networking**.
3. Select a standard switch and click **Properties**.
4. Click the **Ports** tab.
5. To edit the **Failover and Load Balancing** values, select the standard switch item and click **Edit**.

6 Click the **NIC Teaming** tab.

You can override the failover order at the port group level. By default, new adapters are active for all policies. New adapters carry traffic for the standard switch and its port group unless you specify otherwise.

7 In the **Load Balancing** list, select an option for how to select an uplink.

Option	Description
Route based on the originating port ID	Select an uplink based on the virtual port where the traffic entered the standard switch.
Route based on ip hash	Select 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	Select an uplink based on a hash of the source Ethernet.
Use explicit failover order	Always use the highest order uplink from the list of Active adapters that passes failover detection criteria.

8 In the Network failover detection list, select the option to use for failover detection.

Option	Description
Link Status only	Relies solely 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 misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch.
Beacon Probing	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 option detects many of the failures mentioned above that are not detected by link status alone. NOTE Do not use beacon probing with IP-hash load balancing.

9 Select **Yes** or **No** to notify switches in the case of failover.

If you select Yes, whenever a virtual NIC is connected to the standard switch or whenever that virtual NIC's traffic is routed over a different physical NIC in the team because of a failover event, a notification is sent over the network to update the lookup tables on the physical switches. In almost all cases, this is desirable for the lowest latency of failover occurrences and migrations with vMotion.

Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing (NLB) in unicast mode. No such issue exists with NLB running in multicast mode.

10 Select **Yes** or **No** 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**, the adapter is returned to active duty immediately on 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 active adapter fails, requiring its replacement.

11 Set **Failover Order** to specify how to distribute the work load for adapters.

To use some adapters but reserve others for emergencies, you can set this condition using the drop-down menu to place them into groups.

Option	Description
Active Adapters	Continue to use the adapter when the network adapter connectivity is available and active.
Standby Adapters	Use this adapter if one of the active adapter's connectivity is unavailable.
Unused Adapters	Do not use this adapter.

If you are using iSCSI Multipathing, your VMkernel interface must be configured to have one active adapter and no standby adapters. See the *vSphere Storage* documentation.

NOTE When using IP-hash load balancing, do not configure standby uplinks.

Edit the Failover and Load Balancing Policy on a Standard Port Group

Failover and load balancing policies allow you to determine how network traffic is distributed between adapters and how to re-route traffic in the event of an adapter failure.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select a standard switch and click **Properties**.

4 On **Ports** tab, select a port group and click **Edit**.

5 Click the **NIC Teaming** tab.

You can override the failover order at the port-group level. By default, new adapters are active for all policies. New adapters carry traffic for the standard switch and its port group unless you specify otherwise.

6 Specify the settings in the Policy Exceptions group.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Route based on the originating port ID**. Choose an uplink based on the virtual port where the traffic entered the 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. ■ **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 that the physical switch be configured with etherchannel. For all other options, etherchannel should be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ **Link Status only**. Relies solely 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 Probing**. 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.
Notify Switches	Select **Yes** or **No** to notify switches in the case of failover. If you select **Yes**, whenever a virtual NIC is connected to the standard switch or whenever that virtual NIC's traffic would 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.
Failback	Select **Yes** or **No** 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 connectivity is down. ■ **Unused Uplinks**. Do not use this uplink.

7 Click **OK**.

Edit the Teaming and Failover Policy on a Distributed Port Group

Teaming and Failover policies allow you to determine how network traffic is distributed between adapters and how to re-route traffic in the event of an adapter failure.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 In the Teaming and Failover group specify the following.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Route based on the originating virtual port** — Choose an uplink based on the virtual port where the traffic entered the distributed 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 physical NIC load** — Choose an uplink based on the current loads of physical NICs. ■ **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 that the physical switch be configured with etherchannel. For all other options, etherchannel should be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ **Link Status only** – Relies solely 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 Probing** – 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** or **No** 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 would 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** or **No** 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 connectivity is down. ■ **Unused Uplinks** — Do not use this uplink. **Note** When using IP-hash load balancing, do not configure standby uplinks.

5 Click **OK**.

Edit Distributed Port Teaming and Failover Policies

Teaming and Failover policies allow you to determine how network traffic is distributed between adapters and how to re-route traffic in the event of an adapter failure.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **Policies** to view and modify port networking policies.

5 In the Teaming and Failover group, specify the following.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Route based on the originating virtual port** — Choose an uplink based on the virtual port where the traffic entered the vSphere distributed 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 physical NIC load** — Choose an uplink based on the current loads of physical NICs. ■ **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 that the physical switch be configured with etherchannel. For all other options, etherchannel should be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ **Link Status only** – Relies solely 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 Probing** – 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 choose beacon probing with IP-hash load balancing.
Notify Switches	Select **Yes** or **No** to notify switches in the case of failover. If you select **Yes**, whenever a virtual NIC is connected to the vSphere distributed switch or whenever that virtual NIC's traffic would 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.
Failback	Select **Yes** or **No** 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 connectivity is down. NOTE When using IP-hash load balancing, do not configure standby uplinks. ■ **Unused Uplinks** — Do not use this uplink.

6 Click **OK**.

VLAN Policy

VLAN policies determine how VLANs function across your network environment.

A virtual local area network (VLAN) is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if not on the same network switch.

The scope of VLAN policies can be distributed port groups and ports, and uplink port groups and ports.

Edit the VLAN Policy on a Distributed Port Group

The VLAN policy allows virtual networks to join physical VLANs.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 Select the type of VLAN filtering and marking from the **VLAN Type** drop-down menu.

Option	Description
None	Do not use VLAN. Use this option in case of External Switch Tagging (EST).
VLAN	Tag traffic with the ID from the **VLAN ID** field. Type a number between 1 and 4094 for Virtual Switch Tagging (VST).
VLAN Trunking	Pass VLAN traffic with ID within the **VLAN trunk range** to guest operating system. You can set multiple ranges and individual VLANs by using a comma-separated list. Use this option for VGT.
Private VLAN	Associate the traffic with a private VLAN created on the distributed switch.

5 Click **OK**.

Edit Distributed Port or Uplink Port VLAN Policies

The VLAN policy allows virtual networks to join physical VLANs.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **Policies**.

5 Select the **VLAN Type** to use.

Option	Action
None	Do not use VLAN.
VLAN	In the **VLAN ID** field, enter a number between 1 and 4094.
VLAN Trunking	Enter one or more **VLAN trunk range**.
Private VLAN	Select an available private VLAN to use.

6 Click **OK**.

Edit the VLAN Policy on an Uplink Port Group

Set the VLAN policy on an uplink port group with the vSphere Client to configure VLAN traffic processing generally for all member uplinks.

Use the VLAN policy at the uplink port level to propagate a trunk range of VLAN IDs to the physical network adapters for traffic filtering. The physical network adapters drop the packets from the other VLANs if the adapters support filtering by VLAN. Setting a trunk range improves networking performance because physical network adapters filter traffic instead of the uplink ports in the group.

If you have a physical network adapter which does not support VLAN filtering, the VLANs might still not be blocked. In this case, configure VLAN filtering on a distributed port group or on a distributed port.

See the technical documentation from the adapter vendors for information about VLAN filtering support.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the uplink port group in the inventory pane, and select **Edit Settings**.

3 Under **Policies**, click **VLAN** and type a **VLAN trunk range** to propagate to the physical network adapters.

   For trunking of several ranges and individual VLANs, separate the entries with commas.

4 Click **OK**.

Edit the VLAN Policy on an Uplink Port

Set the VLAN policy on an uplink port with the vSphere Client to handle VLAN traffic through the port in a different way than for the parent uplink port group.

Use the VLAN policy at the uplink port to propagate a trunk range of VLAN IDs to the physical network adapter for traffic filtering. The physical network adapter drops packets from the other VLANs if the adapter supports filtering by VLAN. Setting a trunk range improves networking performance because the physical network adapter filters traffic instead of the uplink port.

If you have a physical network adapter which does not support VLAN filtering, the VLANs might still not be blocked. In this case, configure VLAN filtering on a distributed port group or on a distributed port.

See the technical documentation from the adapter vendor for information about VLAN filtering support.

Launch the vSphere Client and log in to a vCenter Server system.

Prerequisites

To override the VLAN policy at the port level, enable the port-level overrides. See "Edit Advanced Distributed Port Group Settings," on page 44.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Under **Policies**, select **VLAN** and click **Override**.

5 Type a **VLAN trunk range** to propagate to the physical network adapter.

   For trunking of several ranges and individual VLANs, separate the entries with commas.

6 Click **OK**.

Security Policy

Networking security policy provides protection of traffic against MAC address impersonation and unwanted port scanning

The security policy of a standard or distributed switch is implemented in Layer 2 (Data Link Layer) of the network protocol stack. The three elements of the security policy are promiscuous mode, MAC address changes, and forged transmits. See the *vSphere Security* documentation for information about potential networking threats.

Edit Security Policy for a vSphere Standard Switch

You can edit Layer 2 security policies, such as MAC address changes and forged transmits, for a vSphere standard switch.

Layer 2 is the data link layer. The three elements of the Layer 2 Security policy are promiscuous mode, MAC address changes, and forged transmits. In non-promiscuous mode, a guest adapter listens to traffic only on its own MAC address. In promiscuous mode, it can listen to all the packets. By default, guest adapters are set to non-promiscuous mode.

You can override the switch-level settings for individual standard port groups by editing the settings for the port group.

For more information about security, see the *vSphere Security* documentation.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Click **Properties** for the standard switch whose Layer 2 Security policy you want to edit.

4 In the Properties dialog box for the standard switch, click the **Ports** tab.

5 Select the standard switch item and click **Edit**.

6 Click the **Security** tab.

7 In the Policy Exceptions pane, select whether to reject or accept the Layer 2 Security policy exceptions.

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 standard switch that are allowed under the VLAN policy for the port group that the adapter is connected to.
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 OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. ■ **Accept** — Changing the MAC address from the Guest OS has the intended effect: frames to the new MAC address are received.
Forged Transmits	■ **Reject** — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. ■ **Accept** — No filtering is performed and all outbound frames are passed.

8 Click **OK**.

Edit the Layer 2 Security Policy Exception for a Standard Port Group

Control how inbound and outbound frames are handled by editing Layer 2 Security policies.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Choose the vSphere Standard Switch view and click **Properties** for the port group to edit.

4 In the Properties dialog box, click the **Ports** tab.

5 Select the port group item and click **Edit**.

6 In the Properties dialog box for the port group, click the **Security** tab.

By default, **Promiscuous Mode** is set to **Reject**. **MAC Address Changes** and **Forged Transmits** are set to **Accept**.

The policy exception overrides any policy set at the standard switch level.

7 In the Policy Exceptions pane, select whether to reject or accept the security policy exceptions.

Table 22-3. Policy Exceptions

Mode	Reject	Accept
Promiscuous Mode	Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter.	Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the standard switch that are allowed under the VLAN policy for the port group that the adapter is connected to.
MAC Address Changes	If the guest OS 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 OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are sent again.	If the MAC address from the guest OS changes, frames to the new MAC address are received.
Forged Transmits	Outbound frames with a source MAC address that is different from the one set on the adapter are dropped.	No filtering is performed, and all outbound frames are passed.

8 Click **OK**.

Edit the Security Policy for a Distributed Port Group

You can set a security policy on a distributed port group to override the policy set for the distributed switch.

The three elements of the Security policy are promiscuous mode, MAC address changes, and forged transmits.

In nonpromiscuous mode, a guest adapter listens to traffic only on its own MAC address. In promiscuous mode, it can listen to all the packets. By default, guest adapters are set to non-promiscuous mode.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

By default, **Promiscuous Mode** is set to **Reject**. **MAC Address Changes** and **Forced Transmits** are set to **Accept**.

4 In the **Security** group, select whether to reject or accept the Security policy exceptions.

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 standard switch that are allowed under the VLAN policy for the port group that the adapter is connected to.
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 OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. ■ **Accept** — Changing the MAC address from the Guest OS has the intended effect: frames to the new MAC address are received.
Forged Transmits	■ **Reject** — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. ■ **Accept** — No filtering is performed and all outbound frames are passed.

5 Click **OK**.

Edit Distributed Port Security Policies

The three elements of the Security policy are promiscuous mode, MAC address changes, and forged transmits.

In nonpromiscuous mode, a guest adapter listens to traffic only on its own MAC address. In promiscuous mode, it can listen to all the packets. By default, guest adapters are set to non-promiscuous mode.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **Policies**.

By default, **Promiscuous Mode** is set to **Reject**, **MAC Address Changes**, and **Forged Transmits** are set to **Accept**.

5 In the **Security** group, select whether to reject or accept the Security policy exceptions.

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.
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 OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. ■ **Accept** — Changing the MAC address from the Guest OS has the intended effect: frames to the new MAC address are received.
Forged Transmits	■ **Reject** — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. ■ **Accept** — No filtering is performed and all outbound frames are passed.

6 Click **OK**.

Traffic Shaping Policy

A traffic shaping policy is defined by average bandwidth, peak bandwidth, and burst size. You can establish a traffic shaping policy for each port group and each distributed port or distributed port group.

ESXi shapes outbound network traffic on standard switches and inbound and outbound traffic on distributed switches. Traffic shaping restricts the network bandwidth available on a port, but can also be configured to allow bursts of traffic to flow through at higher speeds.

Average Bandwidth Establishes the number of bits per second to allow across a port, averaged over time. This number is the allowed average load.

Peak Bandwidth Maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This number limits the bandwidth that a port uses when it is using its burst bonus.

Burst Size Maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus if it does not use all its allocated bandwidth. When the port needs more bandwidth than specified by the average bandwidth, it might be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter limits the number of bytes that have accumulated in the burst bonus and transfers traffic at a higher speed.

Edit the Traffic Shaping Policy for a vSphere Standard Switch

ESXi allows you to shape outbound traffic on standard switches. The traffic shaper restricts the network bandwidth available to any port, but may also be configured to temporarily allow "bursts" of traffic to flow through a port at higher speeds.

A traffic shaping policy is defined by three characteristics: average bandwidth, peak bandwidth, and burst size.

Average Bandwidth Establishes the number of bits per second to allow across a port, averaged over time—the allowed average load.

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 thus transferred at a higher speed.

Peak Bandwidth The maximum number of bits per second to allow across a port when it is sending a burst of traffic. This tops the bandwidth used by a port whenever it is using its burst bonus. This parameter can never be smaller than the average bandwidth.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab and click **Networking**.

3 Select a standard switch and click **Properties**.

4 Click the **Ports** tab.

5 Select the standard switch and click **Edit**.

6 Click the **Traffic Shaping** tab.

7 Select **Enabled** from the **Status** drop-down menu to enable traffic shaping policy exceptions.

   The Status policy here is applied to each virtual adapter attached to the port group, not to the standard switch as a whole. If you enable the policy exception in the **Status** field, you set limits on the amount of networking bandwidth allocation for each virtual adapter associated with this particular port group. If you disable the policy, services have a clear connection to the physical network by default.

8 For each traffic shaping policy, enter a bandwidth value.

Edit the Traffic Shaping Policy for a Standard Port Group

Use traffic shaping policies to control the bandwidth and burst size on a port group.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 On the host **Configuration** tab, click **Networking**.

3 Choose the vSphere Standard Switch view and click **Properties** for the port group to edit.

4 In the Properties dialog box, click the **Ports** tab.

5 Select the port group item and click **Edit**.

6 In the Properties dialog box for the port group, click the **Traffic Shaping** tab.

When traffic shaping is disabled, the options are dimmed.

Option	Description
Status	If you enable the policy exception in the **Status** field, you are setting limits on the amount of networking bandwidth allocated for each virtual adapter associated with this particular port group. If you disable the policy, services have a free and clear connection to the physical network.
Average Bandwidth	A value measured over a particular period of time.
Peak Bandwidth	Limits the maximum bandwidth during a burst. It can never be smaller than the average bandwidth.
Burst Size	Specifies how large a burst can be in kilobytes (KB).

Edit the Traffic Shaping Policy for a Distributed Port Group

ESXi allows you to shape both inbound and outbound traffic on vSphere distributed switches. The traffic shaper restricts the network bandwidth available to any port, but may also be configured to temporarily allow "bursts" of traffic to flow through a port at higher speeds.

A traffic shaping policy is defined by three characteristics: average bandwidth, peak bandwidth, and burst size.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 In the **Traffic Shaping** group, you can configure both **Ingress Traffic Shaping** and **EgressTraffic Shaping**.

When traffic shaping is disabled, the tunable features are dimmed.

Status — If you enable the policy exception for either **Ingress Traffic Shaping** or **Egress Traffic Shaping** in the **Status** field, you are setting limits on the amount of networking bandwidth allocated for each virtual adapter associated with this particular port group. If you disable the policy, services have a free, clear connection to the physical network by default.

5 Specify network traffic 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/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 thus transferred at a higher speed.

6 Click **OK**.

Edit Distributed Port or Uplink Port Traffic Shaping Policies

ESXi allows you to shape both inbound and outbound traffic on vSphere distributed switches. The traffic shaper restricts the network bandwidth available to any port, but may also be configured to temporarily allow "bursts" of traffic to flow through a port at higher speeds.

A traffic shaping policy is defined by three characteristics: average bandwidth, peak bandwidth, and burst size.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **Policies**.

5 In the **Traffic Shaping** group, you can configure both **Inbound Traffic Shaping** and **Outbound Traffic Shaping**.

When traffic shaping is disabled, the tunable features are dimmed.

Status — If you enable the policy exception for either **Inbound Traffic Shaping** or **Outbound Traffic Shaping** in the **Status** field, you are setting limits on the amount of networking bandwidth allocated for each virtual adapter associated with this particular port group. If you disable the policy, services have a free, clear connection to the physical network by default.

6 Specify network traffic parameters.

- **Average Bandwidth** establishes the number of bits per second to allow across a port, averaged over time—the allowed average load.
- **Peak Bandwidth** is the maximum number of bits per second to allow across a port when it is sending/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 thus transferred at a higher speed.

7 Click **OK**.

Resource Allocation Policy

The Resource Allocation policy allows you to associate a distributed port or port group with a user-created network resource pool. This policy provides you with greater control over the bandwidth given to the port or port group.

For information about creating and configuring network resource pools, see "vSphere Network I/O Control," on page 247.

Edit the Resource Allocation Policy on a Distributed Port Group

Associate a distributed port group with a network resource pool to give you greater control over the bandwidth given to the distributed port group.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Enable Network I/O Control on the host and create one or more user-defined network resource pools.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 In the Resource Allocation group, select the **Network Resource Pool** to associate the distributed port group with from the drop-down menu.

5 Click **OK**.

Edit the Resource Allocation Policy on a Distributed Port

Associate a distributed port with a network resource pool to give you greater control over the bandwidth given to the port.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Enable Network I/O Control on the host and create one or more user-defined network resource pools.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Select **Policies**.

5 In the Resource Allocation group, select the **Network Resource Pool** to associate the port with from the drop-down menu.

6 Click **OK**.

Monitoring Policy

The monitoring policy enables or disables NetFlow monitoring on a distributed port or port group.

NetFlow settings are configured at the vSphere distributed switch level. See "Configure NetFlow Settings," on page 293.

Edit the Monitoring Policy on a Distributed Port Group

With the Monitoring policy, you can enable or disable NetFlow monitoring on a distributed port group.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 In the Monitoring group, select the **NetFlow status**.

Option	Description
Disabled	NetFlow is disabled on the distributed port group.
Enabled	NetFlow is enabled on the distributed port group. You can configure NetFlow settings at the vSphere distributed switch level. See "Configure NetFlow Settings," on page 293.

5 Click **OK**.

Edit the Monitoring Policy on a Distributed Port

With the Monitoring policy, you can enable or disable NetFlow monitoring on a distributed port.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Select **Policies**.

5 In the Monitoring group, select **NetFlow status**.

Option	Description
Disabled	NetFlow is disabled on the port.
Enabled	NetFlow is enabled on the port. You can configure NetFlow settings at the distributed switch level. See "Configure NetFlow Settings," on page 293.

6 Click **OK**.

Port Blocking Policies

Port blocking policies allow you to selectively block ports from sending or receiving data.

Edit the Port Blocking Policy for a Distributed Port Group

The Miscellaneous policies dialog allows you to configure various distributed port group policies.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed port group in the inventory pane, and select **Edit Settings**.

3 Select **Policies**.

4 In the **Miscellaneous** group, choose whether to **Block all ports** in this distributed port group.

5 Click **OK**.

Edit Distributed Port or Uplink Port Blocking Policies

The Miscellaneous policies dialog allows you to configure distributed port or uplink port blocking policies.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Select the vSphere distributed switch in the inventory pane.

3 On the **Ports** tab, right-click the port to modify and select **Edit Settings**.

4 Click **Policies**.

5 In the **Miscellaneous** group, select whether to **Block** this port.

6 Click **OK**.

Manage Policies for Multiple Port Groups on a vSphere Distributed Switch

You can modify networking policies for multiple port groups on a distributed switch.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.

- Create a vSphere distributed switch with one or more port groups.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the distributed switch and select **Manage Port Groups**.

3 Select the policy categories to modify.

Option	Description
Security	Set MAC address changes, forged transmits, and promiscuous mode for the selected port groups.
Traffic Shaping	Set the average bandwidth, peak bandwidth, and burst size for inbound and outband traffic on the selected port groups.
VLAN	Configure how the selected port groups connect to physical VLANs.
Teaming and Failover	Set load balancing, failover detection, switch notification, and failover order for the selected port groups.
Resource Allocation	Set network resource pool association for the selected port groups. This option is available for vSphere distributed switch versions 5.0.0 and later only.
Monitoring	Enable or disable NetFlow on the selected port groups. This option is available for vSphere distributed switch versions 5.0.0 and later only.
Miscellaneous	Enable or disable port blocking on the selected port groups.

4 Click **Next**.

5 Select one or more port groups to modify and click **Next**.

The policy configuration page appears. Only the policy categories you previously selected are displayed.

6 (Optional) In the Security group, select whether to reject or accept the Security policy exceptions.

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.
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 OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. ■ **Accept** — Changing the MAC address from the Guest OS has the intended effect: frames to the new MAC address are received.
Forged Transmits	■ **Reject** — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. ■ **Accept** — No filtering is performed and all outbound frames are passed.

7 (Optional) In the Traffic Shaping group, you can configure both **Ingress Traffic Shaping** and **Egress Traffic Shaping**.

When traffic shaping is disabled, the tunable features are dimmed.

Status — If you enable the policy exception for either **Ingress Traffic Shaping** or **Egress Traffic Shaping** in the **Status** field, you are setting limits on the amount of networking bandwidth allocated for each distributed port associated with the selected port groups. If you disable the policy, the amount of network bandwidth is not limited before it reaches the physical network .

8 (Optional) Specify network traffic 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/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 thus transferred at a higher speed.

9 (Optional) Select the VLAN Type to use.

Option	Description
None	Do not use VLAN.
VLAN	In the **VLAN ID** field, enter a number between 1 and 4094.
VLAN Trunking	Enter a **VLAN trunk range**.
Private VLAN	Select an available private VLAN to use.

10 (Optional) In the Teaming and Failover group specify the following.

Option	Description
Load Balancing	Specify how to choose an uplink. ■ **Route based on the originating virtual port** — Choose an uplink based on the virtual port where the traffic entered the distributed 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 physical NIC load** — Choose an uplink based on the current loads of physical NICs. ■ **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 that the physical switch be configured with etherchannel. For all other options, etherchannel should be disabled.
Network Failover Detection	Specify the method to use for failover detection. ■ **Link Status only** – Relies solely 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 Probing** – 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** or **No** 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 would 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.
Failback	Select **Yes** or **No** 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 connectivity is down. ■ **Unused Uplinks** — Do not use this uplink. NOTE When using IP-hash load balancing, do not configure standby uplinks.

11 (Optional) In the Resource Allocation group, choose the **Network Resource Pool** to associate the distributed port group with from the drop-down menu.

12 (Optional) In the Monitoring group, choose the **NetFlow status**.

Option	Description
Disabled	NetFlow is disabled on the distributed port group.
Enabled	NetFlow is enabled on the distributed port group. NetFlow settings can be configured at the vSphere distributed switch level.

13 (Optional) In the **Miscellaneous** group, choose whether to **Block all ports** in this distributed port group.

14 Click **Next**.

All displayed policies are applied to all selected port groups, inculding those policies that have not been changed.

15 (Optional) If you need to make any changes, click **Back** to the appropriate screen.

16 Review the port group settings and click **Finish**.

Advanced Networking 23

Advanced networking configuration options allow you greater control over your vSphere networking environment.

This chapter includes the following topics:

- "Internet Protocol Version 6 (IPv6) Support," on page 285
- "VLAN Configuration," on page 286
- "Working With Port Mirroring," on page 286
- "Configure NetFlow Settings," on page 293
- "Switch Discovery Protocol," on page 293
- "Change the DNS and Routing Configuration," on page 295
- "MAC Address Management," on page 296

Internet Protocol Version 6 (IPv6) Support

Internet Protocol version 6 (IPv6) support in ESXi provides the ability to use Virtual Infrastructure features such as NFS in an IPv6 environment. Use the Networking Properties dialog box to enable or disable IPv6 support on the host.

IPv6 is designated by the Internet Engineering Task Force as the successor to IPv4. The most obvious difference is address length. IPv6 uses 128-bit addresses rather than the 32-bit addresses used by IPv4. This increase resolves the problem of address exhaustion and eliminates the need for network address translation. Other differences include link-local addresses that appear as the interface is initialized, addresses that are set by router advertisements, and the ability to have multiple IPv6 addresses on an interface.

In VMware ESXi 5.1, IPv6 is enabled by default.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Host.Configuration.Network Configuration**

Procedure

1 From the vSphere Client Home page, click **Hosts and Clusters**.

2 Select the host and click the **Configuration** tab.

3 Click the **Networking** link under **Hardware**.

4 In the **vSphere Standard Switch** view, click the **Properties** link.

5 Select **Enable IPv6 support on this host** and click **OK**.

6 Reboot the host.

VLAN Configuration

Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments.

Configuring ESXi with VLANs is recommended for the following reasons.

- It integrates the host into a pre-existing environment.
- It isolates and secures network traffic.
- It reduces network traffic congestion.

You can configure VLANs in ESXi using three methods: External Switch Tagging (EST), Virtual Switch Tagging (VST), and Virtual Guest Tagging (VGT).

With EST, all VLAN tagging of packets is performed on the physical switch. Host network adapters are connected to access ports on the physical switch. Port groups that are connected to the virtual switch must have their VLAN ID set to 0.

With VST, all VLAN tagging of packets is performed by the virtual switch before leaving the host. Host network adapters must be connected to trunk ports on the physical switch. Port groups that are connected to the virtual switch must have a VLAN ID between 1 and 4094.

With VGT, all VLAN tagging is done by the virtual machine. VLAN tags are preserved between the virtual machine networking stack and external switch when frames pass to and from virtual switches. Host network adapters must be connected to trunk ports on the physical switch. For a standard switch the VLAN ID of port groups with VGT must be set to 4095. For a distributed switch the VLAN trunking policy must include the range of the VLANs to which virtual machines are connected.

NOTE When using VGT, you must have an 802.1Q VLAN trunking driver installed on the virtual machine.

Working With Port Mirroring

Port mirroring allows you to mirror a distributed port's traffic to other distributed ports or specific physical switch ports.

Port mirroring is used on a switch to send a copy of packets seen on one switch port (or an entire VLAN) to a monitoring connection on another switch port. Port mirroring is used to analyze and debug data or diagnose errors on a network.

Port Mirroring Version Compatibility

Certain port mirroring functionality in vSphere 5.1 and later depends on which version of vCenter Server, vSphere distributed switch, and host you use, and how you use these aspects of vSphere together.

Table 23-1. Port mirroring compatibility

vCenter Server version	vSphere distributed switch version	Host version	vSphere 5.1 port mirroring functionality
vSphere 5.1 and later	vSphere 5.1 and later	vSphere 5.1 and later	vSphere 5.1 port mirroring is available for use. Features for vSphere 5.0 and earlier port mirroring are not available.
vSphere 5.1 and later	vSphere 5.1 and later	vSphere 5.0 and earlier	vSphere 5.0 and earlier hosts can be added to vSphere 5.1 vCenter Server, but cannot be added to distributed switches version 5.1 and later.
vSphere 5.1 and later	vSphere 5.0	vSphere 5.0	vSpherevCenter Server version 5.1 and later can configure port mirroring on a vSphere 5.0 distributed switch.
vSphere 5.1 and later	vSphere 5.0	vSphere 5.1 and later	Hosts running vSphere 5.1 can be added to vSphere 5.0 distributed switches and support vSphere 5.0 port mirroring.
vSphere 5.1 and later	Pre-vSphere 5.0	vSphere 5.5 and earlier	Port mirroring is not supported.
vSphere 5.0 and earlier	vSphere 5.0 and earlier	vSphere 5.1	A vSphere 5.1 host cannot be added to vCenter Server 5.0 and earlier.

If you use a host profile with port mirroring settings, the host profile must be adapted to the new version of port mirroring in vSphere 5.1 and later.

Port Mirroring Interoperability

There are some interoperability issues to consider when using vSphere 5.1 port mirroring with other features of vSphere.

vMotion

vMotion functions differently depending on which vSphere 5.1 port mirroring session type you select. During vMotion, a mirroring path could be temporarily invalid, but is restored when vMotion completes.

Table 23-2. vMotion Interoperability with port mirroring

Port mirroring session type	Source and destination	Interoperable with vMotion	Functionality
Distributed Port Mirroring	Non-uplink distributed port source and destination	Yes	Port mirroring between distributed ports can only be local. If the source and destination are on different hosts due to vMotion, mirroring between them will not work. However, if the source and destination move to the same host, port mirroring works.
Remote Mirroring Source	Non-uplink distributed port source	Yes	When a source distributed port is moved from host A to host B, the original mirroring path from the source port to A's uplink is removed on A, and a new mirroring path from the source port to B's uplink is created on B. Which uplink is used is determined by the uplink name specified in session.
	Uplink port destinations	No	Uplinks can not be moved by vMotion.
Remote Mirroring Destination	VLAN source	No	
	Non-uplink distributed port destination	Yes	When a destination distributed port is moved from host A to host B, all original mirroring paths from source VLANs to the destination port are moved from A to B.
Encapsulated Remote Mirroring (L3) Source	Non-uplink distributed port source	Yes	When a source distributed port is moved from host A to host B, all original mirroring paths from the source port to destination IPs are moved from A to B.
	IP destination	No	
Distributed Port Mirroring (legacy)	IP source	No	
	Non-uplink distributed port destination	No	When a destination distributed port is moved from host A to host B, all original mirroring paths from source IPs to the destination port are invalid because the port mirroring session source still sees the destination on A.

TSO and LRO

TCP Segmentation Offload (TSO) and large receive offload (LRO) might cause the number of mirroring packets to not equal to the number of mirrored packets.

When TSO is enabled on a vNIC, the vNIC might send a large packet to a distributed switch. When LRO is enabled on a vNIC, small packets sent to it might be merged into a large packet.

Source	Destination	Description
TSO	LRO	Packets from the source vNIC might be large packets, and whether they are split is determined by whether their sizes are larger than the destination vNIC LRO limitation.
TSO	Any destination	Packets from the source vNIC might be large packets, and they are split to standard packets at the destination vNIC.
Any source	LRO	Packets from the source vNIC are standard packets, and they might be merged into larger packets at the destination vNIC.

Create a Port Mirroring Session with the vSphere Client

Create a port mirroring session to mirror vSphere distributed switch traffic to specific physical switch ports.

Prerequisites

Create a vSphere distributed switch version 5.0.0 or later.

Procedure

1 Specify Port Mirroring Name and Session Details on page 289

Specify the name, description, and session details for the new port mirroring session.

2 Choose Port Mirroring Sources on page 290

Select sources and traffic direction for the new port mirroring session.

3 Choose Port Mirroring Destinations on page 290

Select ports or uplinks as destinations for the port mirroring session.

4 Verify New Port Mirroring Settings on page 290

Verify and enable the new port mirroring session.

Specify Port Mirroring Name and Session Details

Specify the name, description, and session details for the new port mirroring session.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the Port Mirroring tab, click **Add**.

4 Enter a **Name** and **Description** for the port mirroring session.

5 (Optional) Select **Allow normal IO on destination ports** to allow normal IO traffic on destination ports.

If you do not select this option, mirrored traffic will be allowed out on destination ports, but no traffic will be allowed in.

6 (Optional) Select **Encapsulation VLAN** to create a VLAN ID that encapsulates all frames at the destination ports.

If the original frames have a VLAN and **Preserve original VLAN** is not selected, the encapsulation VLAN replaces the original VLAN.

7 (Optional) Select **Preserve original VLAN** to keep the original VLAN in an inner tag so mirrored frames are double encapsulated.

   This option is available only if you select **Encapsulation VLAN**.

8 (Optional) Select **Mirrored packet length** to put a limit on the size of mirrored frames.

   If this option is selected, all mirrored frames are truncated to the specified length.

9 Click **Next**.

Choose Port Mirroring Sources

Select sources and traffic direction for the new port mirroring session.

Procedure

1 Choose whether to use this source for **Ingress** or **Egress** traffic, or choose **Ingress/Egress** to use this source for both types of traffic.

2 Type the source port IDs and click >> to add the sources to the port mirroring session.

   Separate multiple port IDs with a comma.

3 Click **Next**.

Choose Port Mirroring Destinations

Select ports or uplinks as destinations for the port mirroring session.

Port Mirroring is checked against the VLAN forwarding policy. If the VLAN of the original frames is not equal to or trunked by the destination port, the frames are not mirrored.

Procedure

1 Choose the **Destination type**.

Option	Description
Port	Type in one or more **Port IDs** to use as a destination for the port mirroring session. Separate multiple IDs with a comma.
Uplink	Select one or more uplinks to use as a destination for the port mirroring session.

2 Click >> to add the selected destinations to the port mirroring session.

3 (Optional) Repeat the above steps to add multiple destinations.

4 Click **Next**.

Verify New Port Mirroring Settings

Verify and enable the new port mirroring session.

Procedure

1 Verify that the listed name and settings for the new port mirroring session are correct.

2 (Optional) Click **Back** to make any changes.

3 (Optional) Click **Enable this port mirroring session** to start the port mirroring session immediately.

4 Click **Finish**.

View Port Mirroring Session Details

View port mirroring session details, including status, sources, and destinations.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Port Mirroring** tab, select the port mirroring session to view.

   Details for the selected port mirroring session appear under **Port Mirroring Session Details**.

4 (Optional) Click **Edit** to edit the details for the selected port mirroring session.

5 (Optional) Click **Delete** to delete the selected port mirroring session.

6 (Optional) Click **Add** to add a new port mirroring session.

Edit Port Mirroring Name and Session Details

Edit the details of a port mirroring session, including name, description, and status.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Port Mirroring** tab, select the port mirroring session to modify and click **Edit**.

4 Click the **Properties** tab.

5 (Optional) Type a new **Name** for the port mirroring session.

6 (Optional) Type a new **Description** for the port mirroring session.

7 Select whether the port mirroring session should be **Enabled** or **Disabled**.

8 (Optional) Select **Allow normal IO on destination ports** to allow normal IO traffic on destination ports.

   If you do not select this option, mirrored traffic is allowed out on destination ports, but no traffic is allowed in.

9 (Optional) Select **Encapsulation VLAN** to create a VLAN ID that encapsulates all frames at the destination ports.

   If the original frames have a VLAN and **Preserve original VLAN** is not selected, the encapsulation VLAN replaces the original VLAN.

10 (Optional) Select **Preserve original VLAN** to keep the original VLAN in an inner tag so mirrored frames are double encapsulated.

   This option is available only if you select **Encapsulation VLAN**.

11 (Optional) Select **Mirrored packet length** to put a limit on the size of mirrored frames.

   If this option is selected, all mirrored frames are truncated to the specified length.

12 Click **OK**.

Edit Port Mirroring Sources

Edit sources and traffic direction for the port mirroring session.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Port Mirroring** tab, select the port mirroring session to modify and click **Edit**.

4 Click the **Sources** tab.

5 (Optional) Select whether to use this source for **Ingress** or **Egress** traffic, or select **Ingress/Egress** to use this source for both types of traffic.

6 (Optional) Type one or more port IDs or ranges of port IDs to add as source for the port mirroring session, and click >>.

   Separate multiple IDs with commas.

7 (Optional) Select a source in the right-hand list and click << to remove the source from the port mirroring session.

8 Click **OK**.

Edit Port Mirroring Destinations

Edit the destination ports and uplinks for a port mirroring session to change where traffic for the session is mirrored.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Port Mirroring** tab, select the port mirroring session to modify and click **Edit**.

4 Click the **Destinations** tab.

5 (Optional) Select the **Destination type** of the destination to add.

Option	Description
Port	Type one or more **Port IDs** to use as a destination for the port mirroring session. Separate multiple IDs with a comma.
Uplink	Select one or more uplinks to use as a destination for the port mirroring session.

6 (Optional) Type one or more port IDs or ranges of port IDs to add as a destination for the port mirroring session and click >>.

   Separate multiple IDs with commas.

7 (Optional) Select a destination from the right-hand column and click **<<** to remove the destination from the port mirroring session.

8 Click **OK**.

Configure NetFlow Settings

NetFlow is a network analysis tool that you can use to monitor network monitoring and virtual machine traffic.

NetFlow is available on vSphere distributed switch version 5.0.0 and later.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 Navigate to the **NetFlow** tab.

4 Type the **IP address** and **Port** of the NetFlow collector.

5 Type the **VDS IP address**.

With an IP address to the vSphere distributed switch, the NetFlow collector can interact with the vSphere distributed switch as a single switch, rather than interacting with a separate, unrelated switch for each associated host.

6 (Optional) Use the up and down menu arrows to set the **Active flow export timeout** and **Idle flow export timeout**.

7 (Optional) Use the up and down menu arrows to set the **Sampling rate**.

The sampling rate determines what portion of data NetFlow collects, with the sampling rate number determining how often NetFlow collects the packets. A collector with a sampling rate of 2 collects data from every other packet. A collector with a sampling rate of 5 collects data from every fifth packet.

8 (Optional) Select **Process internal flows only** to collect data only on network activity between virtual machines on the same host.

9 Click **OK**.

Switch Discovery Protocol

Switch discovery protocols help vSphere administrators to determine which port of the physical switch is connected to a vSphere standard switch or vSphere distributed switch.

vSphere 5.0 and later supports Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP). CDP is available for vSphere standard switches and vSphere distributed switches connected to Cisco physical switches. LLDP is available for vSphere distributed switches version 5.0.0 and later.

When CDP or LLDP is enabled for a particular vSphere distributed switch or vSphere standard switch, you can view properties of the peer physical switch such as device ID, software version, and timeout from the vSphere Web Client.

Enable Cisco Discovery Protocol on a vSphere Distributed Switch

Cisco Discovery Protocol (CDP) allows vSphere administrators to determine which Cisco switch port connects to a given vSphere standard switch or vSphere distributed switch. When CDP is enabled for a particular vSphere distributed switch, you can view properties of the Cisco switch (such as device ID, software version, and timeout) from the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Properties** tab, select **Advanced**.

4 Select **Enabled** from the **Status** drop-down menu.

5 Select **Cisco Discovery Protocol** from the **Type** drop-down menu.

6 Select the CDP mode from the **Operation** drop-down menu.

Option	Description
Listen	ESXi detects and displays information about the associated Cisco switch port, but information about the vSphere distributed switch is not available to the Cisco switch administrator.
Advertise	ESXi makes information about the vSphere distributed switch available to the Cisco switch administrator, but does not detect and display information about the Cisco switch.
Both	ESXi detects and displays information about the associated Cisco switch and makes information about the vSphere distributed switch available to the Cisco switch administrator.

7 Click **OK**.

Enable Link Layer Discovery Protocol on a vSphere Distributed Switch

With Link Layer Discovery Protocol (LLDP), vSphere administrators can determine which physical switch port connects to a given vSphere distributed switch. When LLDP is enabled for a particular distributed switch, you can view properties of the physical switch (such as chassis ID, system name and description, and device capabilities) from the vSphere Client.

LLDP is available only on vSphere distributed switch version 5.0.0 and later.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the **Networking** inventory view.

2 Right-click the vSphere distributed switch in the inventory pane, and select **Edit Settings**.

3 On the **Properties** tab, select **Advanced**.

4 Select **Enabled** from the **Status** drop-down menu.

5 Select **Link Layer Discovery Protocol** from the **Type** drop-down menu.

6 Select the LLDP mode from the **Operation** drop-down menu.

Option	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere distributed switch is not available to the switch administrator.
Advertise	ESXi makes information about the vSphere distributed 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 distributed switch available to the switch administrator.

7 Click **OK**.

View Switch Information on the vSphere Client

When CDP or LLDP is set to **Listen** or **Both**, you can view physical switch information from the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Click the information icon to the right of the vSphere standard switch or vSphere distributed switch to display information for that switch.

Switch information for the selected switch appears.

Change the DNS and Routing Configuration

You can change the DNS server and default gateway information provided during installation from the host configuration page in the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab, and click **DNS and Routing**.

3 On the right side of the window, click **Properties**.

4 In the **DNS Configuration** tab, enter a name and domain.

5 Choose whether to obtain the DNS server address automatically or use a DNS server address.

6 Specify the domains in which to look for hosts.

7 On the **Routing** tab, change the default gateway information as needed.

8 Click **OK**.

MAC Address Management

MAC addresses are used in the Layer 2 (Data Link Layer) of the network protocol stack to transmit frames to a recipient. In vSphere, vCenter Server generates MAC addresses for virtual machine adapters and VMkernel adapters, or you can assign addresses manually.

Each network adapter manufacturer is assigned a unique three-byte prefix called an Organizationally Unique Identifier (OUI), which it can use to generate unique MAC addresses.

VMware supports several address allocation mechanisms, each of them with a separate OUI:

- Generated MAC addresses
  - Assigned by vCenter Server
  - Assigned by the ESXi host
- Manually set MAC addresses
- Generated for legacy virtual machines, but no longer used with ESXi

If you reconfigure the network adapter of a powered off virtual machine, for example by changing the automatic MAC address allocation type, or setting a static MAC address, vCenter Server resolves any MAC address conflict before the adapter reconfiguration takes effect.

Add or Adjust Range- or Prefixed-Based Allocations in the vSphere Client

If you use a range- or prefixed-based allocation, you can use the vSphere Client to adjust the parameters of your allocation.

To change allocation schemes from VMware OUI to a range- or prefixed-based allocation, you must add a key and default value to Advanced Settings. If you already added the key and default values, use **Advanced Settings** to adjust the parameters for each key.

To change from a range- or prefixed-based allocation to the VMware OUI allocation, you cannot use the vSphere Client. You must edit the `vpxd.cfg` file manually. VMware recommends changing allocation types through the vSphere Client because editing files can introduce errors. For information about editing the `vpxd.cfg` file, see the *vSphere Networking* publication.

Caution Prefix-based MAC address allocation is only supported invCenter Server 5.1 and 5.1 hosts. If you add pre-5.1 hosts to vCenter Server 5.1 , and use anything other than VMware OUI prefix-based MAC address allocation, virtual machines assigned non-VMware OUI prefixed MAC addresses fail to power on their pre-5.1 hosts.

The prefix-based MAC address allocation schemes are not supported on pre-5.1 hosts because pre-5.1 hosts explicitly validate if an assigned MAC address uses the VMware OUI 00:50:56 prefix. If the MAC address is not prefixed with 00:50:56, the virtual machine pre-5.1 host fails to power on.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client, select **Administration > Server Settings**.
2. Select **Advanced Settings**.

3 Add or adjust one of the following allocation types.

NOTE Use only one allocation type.

- Prefix-based allocation

Key	Default Value
config.vpxd.macAllocScheme.prefixScheme.prefix	005026
config.vpxd.macAllocScheme.prefixScheme.prefixLength	23

Change the default values to your choice of prefix and prefix length.

- Range-based allocation

Key	Default Value
config.vpxd.macAllocScheme.rangeScheme.range[0].begin	005067000000
config.vpxd.macAllocScheme.rangeScheme.range[0].end	005067ffffff

Change the default values to the allocation range of your choice. Replace [0] with the range ID of your choice.

4 Click **OK**.

Assign a static MAC Address in the vSphere Client

You can assign static MAC addresses to a powered-down virtual machine's virtual NICs.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the virtual machine from the inventory panel.

2 Click the **Summary** tab and click **Edit Settings**.

3 Select the network adapter from the Hardware list.

4 In the MAC Address group, select **Manual**.

5 Enter the static MAC address, and click **OK**.

Managing Storage in the vSphere Client

24

When you connect to a host or vCenter Server using the vSphere Client, you can perform a variety of storage management tasks, including configuring adapters, creating datastores, and viewing storage device information.

This chapter includes the following topics:

- "Storage Limitations in the vSphere Client," on page 300
- "Display Storage Devices for a Host in the vSphere Client," on page 300
- "Display Storage Devices for an Adapter in the vSphere Client," on page 301
- "View Storage Adapters Information in the vSphere Client," on page 301
- "Review Datastore Information in the vSphere Client," on page 301
- "Assign WWNs to Virtual Machines," on page 301
- "Modify WWN Assignments," on page 302
- "Set Up Networking for Software FCoE," on page 303
- "Add Software FCoE Adapters," on page 304
- "Disable Automatic Host Registration," on page 304
- "Setting Up Independent Hardware iSCSI Adapters," on page 305
- "Configuring Dependent Hardware iSCSI Adapters," on page 306
- "Configuring Software iSCSI Adapters," on page 308
- "Setting Up iSCSI Network," on page 310
- "Using Jumbo Frames with iSCSI," on page 315
- "Configuring Discovery Addresses for iSCSI Adapters," on page 316
- "Configuring CHAP Parameters for iSCSI Adapters," on page 317
- "Configure Advanced Parameters for iSCSI in the vSphere Client," on page 320
- "Managing Storage Devices," on page 321
- "Working with Datastores," on page 322
- "Raw Device Mapping," on page 332
- "Understanding Multipathing and Failover," on page 333
- "Storage Hardware Acceleration," on page 335

- "Storage Thin Provisioning," on page 336
- "Using Storage Vendor Providers," on page 338

Storage Limitations in the vSphere Client

The storage tasks that you can perform when you connect directly to an ESXi host or vCenter Server system with the vSphere Client are limited.

The following storage features are unavailable or read-only in the vSphere Client:

- AHCI SATA devices
- NFS client 4.1 with Kerberos
- Storage DRS with vSphere Replication
- Storage DRS interoperability with vCenter Site Recovery Manager
- Storage Policy I/O filters
- Virtual SAN disk group management
- Virtual SAN profile compatibility errors and warnings
- Virtual SAN storage policy based management
- Virtual SAN default profiles
- Virtual SAN disk serviceability
- Virtual SAN fault domain isolation
- Virtual Volumes
- vSphere Flash Read Cache
- vSphere Flash Read Cache DRS interoperability

Use the vSphere Web Client as the primary interface for managing the full range of storage functions available in your vSphere 6.0 environment.

Display Storage Devices for a Host in the vSphere Client

Use the vSphere Client to display all storage devices or LUNs available to a host. If you use any third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. Select a host and click the **Configuration** tab.
2. In Hardware, select **Storage**.
3. Click **Devices**.
4. To view additional details about a specific device, select the device from the list.

Display Storage Devices for an Adapter in the vSphere Client

Use the vSphere Client to display a list of storage devices accessible to a specific storage adapter on the host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a host and click the **Configuration** tab.

2 In Hardware, select **Storage Adapters**.

3 Select the adapter from the Storage Adapters list.

4 Click **Devices**.

View Storage Adapters Information in the vSphere Client

Use the vSphere Client to display storage adapters that your host uses and to review their information.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a host and click the **Configuration** tab.

2 In Hardware, select **Storage Adapters**.

3 To view details for a specific adapter, select the adapter from the Storage Adapters list.

4 To list all storage devices the adapter can access, click **Devices**.

5 To list all paths the adapter uses, click **Paths**.

Review Datastore Information in the vSphere Client

Use the vSphere Client to display all datastores available to the hosts and analyze their properties.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a host and click the **Configuration** tab.

2 In Hardware, select **Storage**.

3 Click the **Datastores** view.

4 To display details for a particular datastore, select the datastore from the list.

Assign WWNs to Virtual Machines

You can assign a WWN to a new virtual machine with an RDM disk when you create this virtual machine.

You can create from 1 to 16 WWN pairs, which can be mapped to the first 1 to 16 physical HBAs on the host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Open the New Virtual Machine wizard.

2 Select **Custom**, and click **Next**.

3 Follow all steps required to create a custom virtual machine.

4 On the Select a Disk page, select **Raw Device Mapping**, and click **Next**.

5 From a list of SAN disks or LUNs, select a raw LUN you want your virtual machine to access directly.

6 Select a datastore for the RDM mapping file.

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

   NOTE If you want to use vMotion for a virtual machine with enabled NPIV, make sure that the RDM file is located on the same datastore where the virtual machine configuration file resides.

7 Follow the steps required to create a virtual machine with the RDM.

8 On the Ready to Complete page, select the **Edit the virtual machine settings before completion** check box and click **Continue**.

   The Virtual Machine Properties dialog box opens.

9 Assign WWNs to the virtual machine.

   a Click the **Options** tab, and select **Fibre Channel NPIV**.

   b Select **Generate new WWNs**.

   c Specify the number of WWNNs and WWPNs.

      A minimum of 2 WWPNs are needed to support failover with NPIV. Typically only 1 WWNN is created for each virtual machine.

10 Click **Finish**.

The host creates WWN assignments for the virtual machine.

What to do next

Register newly created WWNs in the fabric so that the virtual machine is able to log in to the switch, and assign storage LUNs to the WWNs.

Modify WWN Assignments

You can modify WWN assignments for a virtual machine with an RDM.

Typically, you do not need to change existing WWN assignments on your virtual machine. In certain circumstances, for example, when manually assigned WWNs are causing conflicts on the SAN, you might need to change or remove WWNs.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Make sure to power off the virtual machine if you want to edit the existing WWNs.

Before you begin, ensure that your SAN administrator has provisioned the storage LUN ACL to allow the virtual machine's ESXi host to access it.

Procedure

1 Open the Virtual Machine Properties dialog box by clicking the **Edit Settings** link for the selected virtual machine.

2 Click the **Options** tab and select **Fibre Channel NPIV**.

The Virtual Machine Properties dialog box opens.

3 Edit the WWN assignments by selecting one of the following options:

Option	Description
Temporarily disable NPIV for this virtual machine	Disable the WWN assignments for the virtual machine.
Leave unchanged	The existing WWN assignments are retained. The read-only WWN Assignments section of this dialog box displays the node and port values of any existing WWN assignments.
Generate new WWNs	New WWNs are generated and assigned to the virtual machine, overwriting any existing WWNs (those of the HBA itself are unaffected).
Remove WWN assignment	The WWNs assigned to the virtual machine are removed and it uses the HBA WWNs to access the storage LUN. This option is not available if you are creating a new virtual machine.

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

Set Up Networking for Software FCoE

Before you activate the software FCoE adapters, you need to connect the VMkernel to physical FCoE NICs installed on your host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 In the vSphere standard switch view, click **Add Networking**.

4 Select **VMkernel** and click **Next**.

5 Select **Create a vSphere standard switch** to create a new vSphere standard switch.

6 Select the network adapter (vmnic#) that supports FCoE and click **Next**.

If your host has multiple network adapters or multiple ports on the adapter, you can add all of them to a single vSphere standard switch. An alternative is to connect each FCoE NIC to a separate standard switch.

NOTE ESXi supports the maximum of four network adapter ports used for software FCoE.

7 Enter a network label.

Network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, FCoE.

8 Specify a VLAN ID and click **Next**.

Because FCoE traffic requires an isolated network, make sure that the VLAN ID you enter is different from the one used for regular networking on your host. For more information, see the *vSphere Networking* documentation.

9 Specify the IP settings and click **Next**.

10 Review the information and click **Finish**.

You have created the virtual VMkernel adapter for the physical FCoE network adapter installed on your host.

NOTE To avoid FCoE traffic disruptions, do not remove the FCoE network adapter (vmnic#) from the vSphere standard switch after you set up FCoE networking.

Add Software FCoE Adapters

You must activate software FCoE adapters so that your host can use them to access Fibre Channel storage.

The number of software FCoE adapters you can activate corresponds to the number of physical FCoE NIC ports on your host. ESXi supports the maximum of four software FCoE adapters on one host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Set up networking for the software FCoE adapter.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

3 Click **Add**, select **Software FCoE Adapter**, and click **OK**.

4 On the Add Software FCoE Adapter dialog box, select an appropriate vmnic from the drop-down list of physical network adapters.

Only those adapters that are not yet used for FCoE traffic are listed.

5 Click **OK**.

The software FCoE adapter appears on the list of storage adapters.

After you activate the software FCoE adapter, you can view its properties. If you do not use the adapter, you can remove it from the list of adapters.

Disable Automatic Host Registration

When you use EMC CLARiiON or Invista arrays for storage, it is required that the hosts register with the arrays. ESXi performs automatic host registration by sending the host's name and IP address to the array. If you prefer to perform manual registration using storage management software, disable the ESXi auto-registration feature.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host in the inventory panel.

2 Click the **Configuration** tab and click **Advanced Settings** under Software.

3 Click **Disk** in the left panel and scroll down to Disk.EnableNaviReg on the right.

4 Change the default value to 0.

This disables the automatic host registration enabled by default.

Setting Up Independent Hardware iSCSI Adapters

An independent hardware iSCSI adapter is a specialized third-party adapter capable of accessing iSCSI storage over TCP/IP. This iSCSI adapter handles all iSCSI and network processing and management for your ESXi system.

When you connect the vSphere Client directly to a host, the setup and configuration process for the independent hardware iSCSI adapters involves these steps:

1 Check whether the adapter needs to be licensed.

   See your vendor documentation.

2 Install the adapter.

   For installation information and information on firmware updates, see vendor documentation.

3 Verity that the adapter is installed correctly.

   See "View Independent Hardware iSCSI Adapters in the vSphere Client," on page 305.

4 Configure discovery information.

   See "Configuring Discovery Addresses for iSCSI Adapters," on page 316.

5 (Optional) Configure CHAP parameters.

   See "Configuring CHAP Parameters for iSCSI Adapters," on page 317.

6 (Optional) Enable Jumbo Frames.

   See "Using Jumbo Frames with iSCSI," on page 315.

View Independent Hardware iSCSI Adapters in the vSphere Client

View an independent hardware iSCSI adapter to verify that it is correctly installed and ready for configuration.

After you install an independent hardware iSCSI adapter, it appears on the list of storage adapters available for configuration. You can view its properties.

Prerequisites

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

   If it is installed, the hardware iSCSI adapter appears on the list of storage adapters.

3 Select the adapter to view.

   The default details for the adapter appear, including the model, iSCSI name, iSCSI alias, IP address, and target and paths information.

4 Click **Properties**.

The iSCSI Initiator Properties dialog box appears. The **General** tab displays additional characteristics of the adapter.

You can now configure your independent hardware adapter or change its default characteristics.

Change Name and IP Address for Independent Hardware iSCSI Adapters

When you configure your independent hardware iSCSI adapters, make sure that their names and IP addresses are formatted properly.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1 Access the iSCSI Initiator Properties dialog box.

2 Click **Configure**.

3 To change the default iSCSI name for your adapter, enter the new name.

Make sure the name you enter is worldwide unique and properly formatted or some storage devices might not recognize the iSCSI adapter.

4 (Optional) Enter the iSCSI alias.

The alias is a name that you use to identify the independent hardware iSCSI adapter.

5 Change the default IP settings.

You must change the default IP settings so that they are configured properly for the IP SAN. Work with your network administrator to determine the IP setting for the HBA.

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

If you change the iSCSI name, it will be used for new iSCSI sessions. For existing sessions, new settings will not be used until logout and re-login.

Configuring Dependent Hardware iSCSI Adapters

A dependent hardware iSCSI adapter is a third-party adapter that depends on VMware networking, and iSCSI configuration and management interfaces provided by VMware.

An example of a dependent iSCSI adapter is a Broadcom 5709 NIC. When installed on a host, it presents its two components, a standard network adapter and an iSCSI engine, to the same port. The iSCSI engine appears on the list of storage adapters as an iSCSI adapter (vmhba). Although the iSCSI adapter is enabled by default, to make it functional, you must first connect it, through a virtual VMkernel adapter (vmk), to a physical network adapter (vmnic) associated with it. You can then configure the iSCSI adapter.

After you configure the dependent hardware iSCSI adapter, the discovery and authentication data are passed through the network connection, while the iSCSI traffic goes through the iSCSI engine, bypassing the network.

The entire setup and configuration process for the dependent hardware iSCSI adapters involves these steps:

1 View the dependent hardware adapters.

See "View Dependent Hardware iSCSI Adapters," on page 307.

If your dependent hardware adapters do not appear on the list of storage adapters, check whether they need to be licensed. See your vendor documentation.

2 Determine the association between the dependent hardware adapters and physical NICs.

See "Determine Association Between iSCSI and Network Adapters," on page 308.

Make sure to note the names of the corresponding physical NICs. For example, the vmhba33 adapter corresponds to vmnic1 and vmhba34 corresponds to vmnic2.

3 Configure networking for iSCSI.

See "Setting Up iSCSI Network," on page 310.

Configuring the network involves creating a VMkernel interface for each physical network adapter and associating the interface with an appropriate iSCSI adapter.

4 (Optional) Enable Jumbo Frames.

See "Using Jumbo Frames with iSCSI," on page 315.

5 Configure discovery information.

See "Configuring Discovery Addresses for iSCSI Adapters," on page 316.

6 (Optional) Configure CHAP parameters.

See "Configuring CHAP Parameters for iSCSI Adapters," on page 317.

View Dependent Hardware iSCSI Adapters

View a dependent hardware iSCSI adapter to verify that it is correctly loaded.

If the dependent hardware adapter does not appear on the list of storage adapters, check whether it needs to be licensed. See your vendor documentation.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

If it is installed, the dependent hardware iSCSI adapter appears on the list of storage adapters under such category as, for example, Broadcom iSCSI Adapter.

3 Select the adapter to view and click **Properties**.

The iSCSI Initiator Properties dialog box opens. It displays the default details for the adapter, including the iSCSI name, iSCSI alias, and the status.

4 (Optional) To change the default iSCSI name, click **Configure**.

What to do next

Although the dependent iSCSI adapter is enabled by default, to make it functional, you must set up networking for the iSCSI traffic and bind the adapter to the appropriate VMkernel iSCSI port. You then configure discovery addresses and CHAP parameters.

Determine Association Between iSCSI and Network Adapters

You create network connections to bind dependent iSCSI and network adapters. To create the connections correctly, you must determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.

Prerequisites

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

Procedure

1 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

2 Click **Add**.

The network adapter, for example vmnic2, that corresponds to the dependent iSCSI adapter is listed.

What to do next

You must bind the associated dependent hardware iSCSI and network adapters by creating the network connections.

Configuring Software iSCSI Adapters

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

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

NOTE Designate a separate network adapter for iSCSI. Do not use iSCSI on 100Mbps or slower adapters.

The software iSCSI adapter configuration workflow includes these steps:

1 Activate the software iSCSI adapter.

See "Activate the Software iSCSI Adapter in the vSphere Client," on page 308.

2 Configure networking for iSCSI.

See "Setting Up iSCSI Network," on page 310.

Configuring the network involves creating a VMkernel interface for each physical network adapter that you use for iSCSI and associating all interfaces with the software iSCSI adapter.

3 (Optional) Enable Jumbo Frames.

See "Using Jumbo Frames with iSCSI," on page 315.

4 Configure discovery information.

See "Configuring Discovery Addresses for iSCSI Adapters," on page 316.

5 (Optional) Configure CHAP parameters.

See "Configuring CHAP Parameters for iSCSI Adapters," on page 317.

Activate the Software iSCSI Adapter in the vSphere Client

You must activate your software iSCSI adapter so that your host can use it to access iSCSI storage.

You can activate only one software iSCSI adapter.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

NOTE If you boot from iSCSI using the software iSCSI adapter, the adapter is enabled and the network configuration is created at the first boot. If you disable the adapter, it is reenabled each time you boot the host.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

3 Click **Add** and select **Software iSCSI Adapter**.

   The software iSCSI adapter appears on the list of storage adapters.

4 Select the iSCSI adapter from the list and click **Properties**.

5 Click **Configure**.

6 Make sure that the adapter is enabled and click **OK**.

   After enabling the adapter, the host assigns the default iSCSI name to it. If you change the default name, follow iSCSI naming conventions.

Disable Software iSCSI Adapter in the vSphere Client

Use the vSphere Client to disable the software iSCSI adapter if you do not need it.

NOTE If you disable the adapter that is used for software iSCSI boot, the adapter is reenabled each time you boot the host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

3 Select the software iSCSI adapter from the list of storage adapters and click **Properties**.

4 Click **Configure**.

5 To disable the adapter, deselect **Enabled** and click **OK**.

6 Reboot the host.

   After reboot, the adapter no longer appears on the list of storage adapters.

The status indicates that the adapter is disabled.

Setting Up iSCSI Network

Software and dependent hardware iSCSI adapters depend on VMkernel networking. If you use the software or dependent hardware iSCSI adapters, you must configure connections for the traffic between the iSCSI component and the physical network adapters.

Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You then associate the VMkernel adapter with an appropriate iSCSI adapter. This process is called port binding.

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

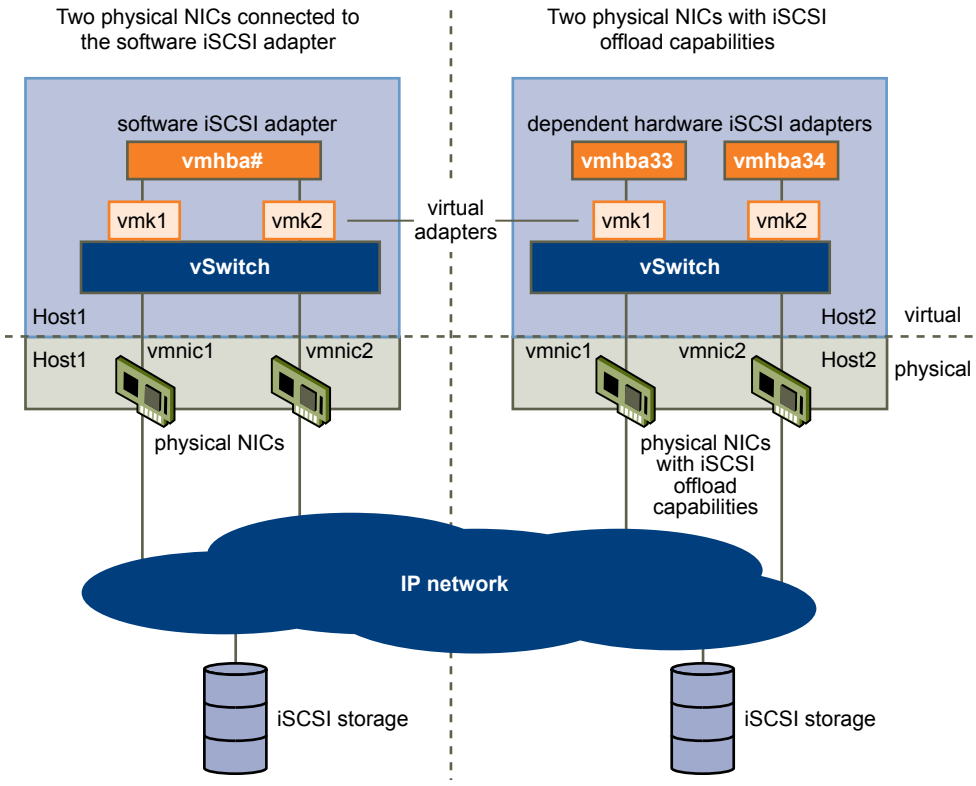
Multiple Network Adapters in iSCSI Configuration

If your host has more than one physical network adapter for software and dependent hardware iSCSI, use the adapters for multipathing.

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

NOTE Physical NICs must be on the same subnet as the iSCSI storage system they connect to.

Figure 24-1. Networking with iSCSI



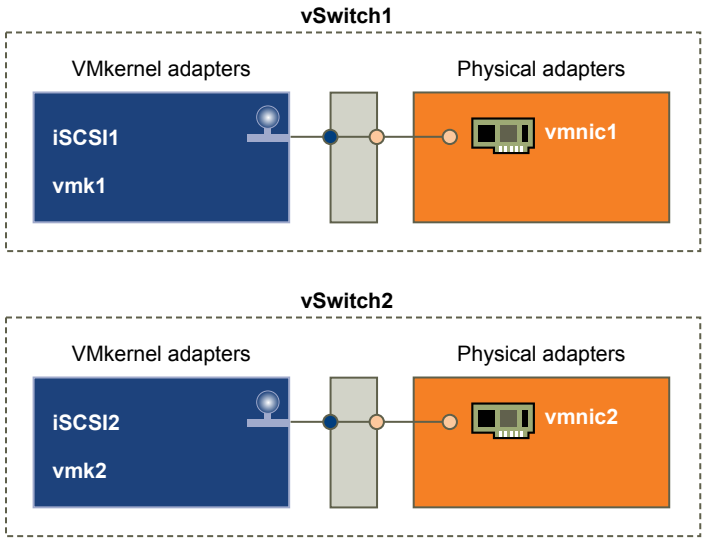
The iSCSI adapter and physical NIC connect through a virtual VMkernel adapter, also called virtual network adapter or VMkernel port. You create a VMkernel adapter (vmk) on a vSphere switch (vSwitch) using 1:1 mapping between each virtual and physical network adapter.

One way to achieve the 1:1 mapping when you have multiple NICs, is to designate a separate vSphere switch for each virtual-to-physical adapter pair.

NOTE If you use separate vSphere switches, you must connect them to different IP subnets. Otherwise, VMkernel adapters might experience connectivity problems and the host will fail to discover iSCSI LUNs.

The following examples show configurations that use vSphere standard switches, but you can use distributed switches as well. For more information about vSphere distributed switches, see the *vSphere Networking* documentation.

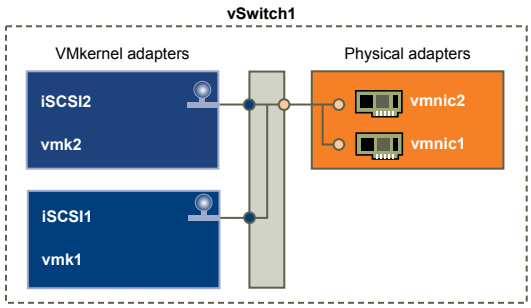
Figure 24-2. 1:1 adapter mapping on separate vSphere standard switches



An alternative is to add all NICs and VMkernel adapters to a single vSphere standard switch. In this case, you must override the default network setup and make sure that each VMkernel adapter maps to only one corresponding active physical adapter.

NOTE You must use the single vSwitch configuration if VMkernel adapters are on the same subnet.

Figure 24-3. 1:1 adapter mapping on a single vSphere standard switch



The following table summarises the iSCSI networking configuration discussed in this topic.

Table 24-1. Networking configuration for iSCSI

iSCSI Adapters	VMkernel Adapters (Ports)	Physical Adapters (NICs)
Software iSCSI		
vmhba32	vmk1	vmnic1
	vmk2	vmnic2
Dependent Hardware iSCSI		

Table 24-1. Networking configuration for iSCSI (Continued)

iSCSI Adapters	VMkernel Adapters (Ports)	Physical Adapters (NICs)
vmhba33	vmk1	vmnic1
vmhba34	vmk2	vmnic2

Create Network Connections for iSCSI in the vSphere Client

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

The following tasks discuss the iSCSI network configuration with a vSphere standard switch.

If you use a vSphere distributed switch with multiple uplink ports, for port binding, create a separate distributed port group per each physical NIC. Then set the team policy so that each distributed port group has only one active uplink port. For detailed information on vSphere distributed switches, see the *vSphere Networking* documentation.

Create a Single VMkernel Adapter for iSCSI

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 In the vSphere Standard Switch view, click **Add Networking**.

4 Select **VMkernel** and click **Next**.

5 Select **Create a vSphere standard switch** to create a new standard switch.

6 Select a NIC to use for iSCSI traffic.

> **Important** If you are creating a VMkernel interface for the dependent hardware iSCSI adapter, select the NIC that corresponds to the iSCSI component. See "Determine Association Between iSCSI and Network Adapters," on page 308.

7 Click **Next**.

8 Enter a network label.

   A network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, iSCSI.

9 Click **Next**.

10 Specify the IP settings and click **Next**.

11 Review the information and click **Finish**.

You created the virtual VMkernel adapter for a physical network adapter on your host.

What to do next

If your host has one physical network adapter for iSCSI traffic, you must bind the virtual adapter that you created to the iSCSI adapter.

If you have multiple network adapters, create additional VMkernel adapters and then perform iSCSI binding. The number of virtual adapters must correspond to the number of physical adapters on the host.

Create Additional VMkernel Adapters for iSCSI

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

You must create a vSphere standard switch that maps an iSCSI VMkernel adapter to a single physical NIC designated for iSCSI traffic.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 Connect additional network adapters to the standard switch.

   a In the standard switch Properties dialog box, click the **Network Adapters** tab and click **Add**.

   b Select one or more NICs from the list and click **Next**.

   With dependent hardware iSCSI adapters, select only those NICs that have a corresponding iSCSI component.

   c Review the information on the Adapter Summary page and click **Finish**.

   The list of network adapters reappears, showing the network adapters that the vSphere standard switch now claims.

5 Create iSCSI VMkernel adapters for all NICs that you added.

   The number of VMkernel interfaces must correspond to the number of NICs on the vSphere standard switch.

   a In the standard switch Properties dialog box, click the **Ports** tab and click **Add**.

   b Select **VMkernel** and click **Next**.

   c Under **Port Group Properties**, enter a network label, for example iSCSI, and click **Next**.

   d Specify the IP settings and click **Next**.

   When you enter the subnet mask, make sure that the NIC is set to the subnet of the storage system it connects to.

   e Review the information and click **Finish**.

CAUTION If the NIC you use with your iSCSI adapter, either software or dependent hardware, is not in the same subnet as your iSCSI target, your host cannot establish sessions from this network adapter to the target.

What to do next

Change the network policy for all VMkernel adapters, so that it is compatible with the network binding requirements. You can then bind the iSCSI VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Change Port Group Policy for iSCSI VMkernel Adapters

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

By default, for each virtual adapter on the vSphere standard switch, all network adapters appear as active. You must override this setup, so that each VMkernel interface maps to only one corresponding active NIC. For example, vmk1 maps to vmnic1, vmk2 maps to vmnic2, and so on.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Create a vSphere standard switch that connects VMkernel with physical network adapters designated for iSCSI traffic. The number of VMkernel adapters must correspond to the number of physical adapters on the vSphere standard switch.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 On the **Ports** tab, select an iSCSI VMkernel adapter and click **Edit**.

5 Click the **NIC Teaming** tab and select **Override switch failover order**.

6 Designate only one physical adapter as active and move all remaining adapters to the **Unused Adapters** category.

7 Repeat Step 4 through Step 6 for each iSCSI VMkernel interface on the vSphere standard switch.

What to do next

After you perform this task, bind the virtual VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Bind iSCSI Adapters with VMkernel Adapters in the vSphere Client

Bind an iSCSI adapter with a VMkernel adapter.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

   The list of available storage adapters appears.

3 Select the software or dependent iSCSI adapter to configure and click **Properties**.

4 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

5 Click **Add** and select a VMkernel adapter to bind with the iSCSI adapter.

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

6 Click **OK**.

   The network connection appears on the list of VMkernel port bindings for the iSCSI adapter.

7 Verify that the network policy for the connection is compliant with the binding requirements.

Using Jumbo Frames with iSCSI

ESXi supports the use of Jumbo Frames with iSCSI.

Jumbo Frames are Ethernet frames with the size that exceeds 1500 Bytes. The maximum transmission unit (MTU) parameter is typically used to measure the size of Jumbo Frames. ESXi allows Jumbo Frames with the MTU up to 9000 Bytes.

When you use Jumbo Frames for iSCSI traffic, the following considerations apply:

- The network must support Jumbo Frames end-to-end for Jumbo Frames to be effective.
- Check with your vendors to ensure your physical NICs and iSCSI HBAs support Jumbo Frames.
- To set up and verify physical network switches for Jumbo Frames, consult your vendor documentation.

The following table explains the level of support that ESXi provides to Jumbo Frames.

Table 24-2. Support of Jumbo Frames

Type of iSCSI Adapters	Jumbo Frames Support
Software iSCSI	Supported
Dependent Hardware iSCSI	Supported. Check with vendor.
Independent Hardware iSCSI	Supported. Check with vendor.

Enable Jumbo Frames for iSCSI

Use the vSphere Client to enable Jumbo Frames for each vSphere standard switch and VMkernel adapter designated for iSCSI traffic.

Enable Jumbo Frames on the Standard switch and VMkernel adapter by changing the maximum transmission units (MTU) parameter.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Click **Properties** for the standard switch you use for iSCSI traffic.

4 On the Ports tab, select the standard switch and click **Edit**.

5 Set the MTU parameter for the standard switch, and click **OK**.

   This step sets the MTU for all physical NICs on that standard switch. The MTU value should be set to the largest MTU size among all NICs connected to the standard switch.

6 On the Ports tab, select the VMkernel adapter and click **Edit**.

7 Set the MTU to match the value configured on the standard switch, and click **OK**.

Configuring Discovery Addresses for iSCSI Adapters

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 Dynamic Discovery in the vSphere Client

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

Launch the vSphere Client and log in to a vCenter Server system.

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

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

   The list of available storage adapters appears.

3 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

   The list of available storage adapters appears.

4 Select the iSCSI initiator to configure, and click **Properties**.

5 Click the **Dynamic Discovery** tab.

6 To add an address for the SendTargets discovery, click **Add**.

7 Type the IP address or DNS name of the storage system and click **OK**.

After your host establishes the SendTargets session with this system, any newly discovered targets appear in the Static Discovery list.

8 To delete a specific SendTargets server, select it and click **Remove**.

After you remove a SendTargets server, it might still appear in the Inheritance field as the parent of static targets. This entry indicates where the static targets were discovered and does not affect the functionality.

What to do next

After configuring Dynamic Discovery for your iSCSI adapter, rescan the adapter.

Set Up Static Discovery in the vSphere Client

With iSCSI initiators, in addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets.

Launch the vSphere Client and log in to a vCenter Server system.

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

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

The list of available storage adapters appears.

3 Select the iSCSI initiator to configure and click **Properties**.

4 Click the **Static Discovery** tab.

The tab displays all dynamically discovered targets and any static targets already entered.

5 To add a target, click **Add** and enter the target's information.

6 To delete a specific target, select the target and click **Remove**.

What to do next

After configuring Static Discovery for your iSCSI adapter, rescan the adapter.

Configuring CHAP Parameters for iSCSI Adapters

Because the IP networks that the iSCSI technology uses to connect to remote targets do not protect the data they transport, you must ensure security of the connection. One of the protocols that iSCSI implements is the Challenge Handshake Authentication Protocol (CHAP), which verifies the legitimacy of initiators that access targets on the network.

CHAP uses a three-way handshake algorithm to verify the identity of your host and, if applicable, of the iSCSI target when the host and target establish a connection. The verification is based on a predefined private value, or CHAP secret, that the initiator and target share.

ESXi supports CHAP authentication at the adapter level. In this case, all targets receive the same CHAP name and secret from the iSCSI initiator. For software and dependent hardware iSCSI adapters, ESXi also supports per-target CHAP authentication, which allows you to configure different credentials for each target to achieve greater level of security.

Set Up CHAP for iSCSI Adapter in the vSphere Client

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

The CHAP name should not exceed 511 alphanumeric characters and the CHAP secret should not exceed 255 alphanumeric characters. Some adapters, for example the QLogic adapter, might have lower limits, 255 for the CHAP name and 100 for the CHAP secret.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

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

Procedure

1. Access the iSCSI Initiator Properties dialog box.
2. On the **General** tab, click **CHAP**.
3. To configure one-way CHAP, under CHAP specify the following:
   a. Select the CHAP security level.
      - Do not use CHAP unless required by target (software and dependent hardware iSCSI only)
      - Use CHAP unless prohibited by target
      - Use CHAP (software and dependent hardware iSCSI only). To configure mutual CHAP, you must select this option.
   b. Specify the CHAP name.

      Make sure that the name you specify matches the name configured on the storage side.
      - To set the CHAP name to the iSCSI initiator name, select **Use initiator name**.
      - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and type a name in the **Name** text box.
   c. Enter a one-way CHAP secret to be used as part of authentication. Use the same secret that you enter on the storage side.
4. To configure mutual CHAP, first configure one-way CHAP by following the directions in Step 3.

   Make sure to select **Use CHAP** as an option for one-way CHAP. Then, specify the following under **Mutual CHAP**:
   a. Select **Use CHAP**.
   b. Specify the mutual CHAP name.
   c. Enter the mutual CHAP secret. Make sure to use different secrets for the one-way CHAP and mutual CHAP.

5 Click **OK**.

6 Rescan the initiator.

If you change the CHAP or mutual CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and log in again.

Set Up CHAP for Target in the vSphere Client

For software and dependent hardware iSCSI adapters, you can configure different CHAP credentials for each discovery address or static target.

When configuring CHAP parameters, make sure that they match the parameters on the storage side. The CHAP name should not exceed 511 and the CHAP secret 255 alphanumeric characters.

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Before setting up CHAP parameters for software and dependent hardware iSCSI, determine whether to configure one-way or mutual CHAP.

- In one-way CHAP, the target authenticates the initiator.
- In mutual CHAP, both the target and initiator authenticate each other. Make sure to use different secrets for CHAP and mutual CHAP.

Procedure

1 Access the iSCSI Initiator Properties dialog box.

2 Select either **Dynamic Discovery** tab or **Static Discovery** tab.

3 From the list of available targets, select a target you want to configure and click **Settings > CHAP**.

4 Configure one-way CHAP in the CHAP area.

   a Deselect **Inherit from parent**.

   b Select one of the following options:

      - Do not use CHAP unless required by target
      - Use CHAP unless prohibited by target
      - Use CHAP. To be able to configure mutual CHAP, you must select this option.

   c Specify the CHAP name.

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

      - To set the CHAP name to the iSCSI initiator name, select **Use initiator name**.
      - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and enter a name in the **Name** field.

   d Enter a one-way CHAP secret to be used as part of authentication. Make sure to use the same secret that you enter on the storage side.

5 To configure mutual CHAP, first configure one-way CHAP by following directions in Step 4.

   Make sure to select **Use CHAP** as an option for one-way CHAP. Then, specify the following in the Mutual CHAP area:

   a Deselect **Inherit from parent**.

   b Select **Use CHAP**.

c Specify the mutual CHAP name.

d Enter the mutual CHAP secret. Make sure to use different secrets for the one-way CHAP and mutual CHAP.

6 Click **OK**.

7 Rescan the initiator.

If you change the CHAP or mutual CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and login again.

Disable CHAP

You can disable CHAP if your storage system does not require it.

If you disable CHAP on a system that requires CHAP authentication, existing iSCSI sessions remain active until you reboot your host, end the session through the command line, or the storage system forces a logout. After the session ends, you can no longer connect to targets that require CHAP.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1 Open the CHAP Credentials dialog box.

2 For software and dependent hardware iSCSI adapters, to disable just the mutual CHAP and leave the one-way CHAP, select **Do not use CHAP** in the Mutual CHAP area.

3 To disable one-way CHAP, select **Do not use CHAP** in the CHAP area.

The mutual CHAP, if set up, automatically turns to **Do not use CHAP** when you disable the one-way CHAP.

4 Click **OK**.

Configure Advanced Parameters for iSCSI in the vSphere Client

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

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

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Access the iSCSI Initiator Properties dialog box.

2 To configure advanced parameters at the initiator level, on the General tab, click **Advanced**. Proceed to Step 4.

3 Configure advanced parameters at the target level.

   At the target level, advanced parameters can be configured only for software and dependent hardware iSCSI adapters.

   a Select either the **Dynamic Discovery** tab or **Static Discovery** tab.

   b From the list of available targets, select a target to configure and click **Settings > Advanced**.

4 Enter any required values for the advanced parameters you want to modify and click **OK** to save your changes.

Managing Storage Devices

Manage local and networked storage device that your ESXi host has access to.

Rename Storage Devices in the vSphere Client

You can change the display name of a storage device. The display name is assigned by the ESXi host based on the storage type and manufacturer.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the host in the vSphere Client inventory.

2 Click the **Configuration** tab.

3 Click **Storage** and then click **Devices**.

4 Right-click the device to rename and select **Rename**.

5 Change the device name to a friendly name.

Perform Storage Rescan in the vSphere Client

When you make changes in your SAN configuration, you might need to rescan your storage. You can rescan all storage available to your host. If the changes you make are isolated to storage accessed through a specific adapter, perform rescan for only this adapter.

Use this procedure if you want to limit the rescan to storage available to a particular host or accessed through a particular adapter on the host. If you want to rescan storage available to all hosts managed by your vCenter Server system, you can do so by right-clicking a datacenter, cluster, or folder that contains the hosts and selecting **Rescan for Datastores**.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select a host and click the **Configuration** tab.

2 Select a rescan option.

Option	Description
Storage	In the Hardware panel, click **Storage**, and click **Rescan All** above the Datastores or Devices panel.
Storage Adapters	In the Hardware panel, click **Storage Adapters**, and click **Rescan All** above the Storage Adapters panel. NOTE You can also right-click an individual adapter and select **Rescan** to rescan just that adapter.

3 Specify extent of rescan.

Option	Description
Scan for New Storage Devices	Rescan all adapters to discover new storage devices. If new devices are discovered, they appear in the device list.
Scan for New VMFS Volumes	Rescan all storage devices to discover new datastores that have been added since the last scan. Any new datastores appear in the datastore list.

Change the Number of Scanned Storage Devices

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

The value of `Disk.MaxLUN` also determines how many LUNs the SCSI scan code attempts to discover 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 0 through 100, you can set the value to 101 to improve device discovery speed on targets that do not support REPORT_LUNS. Lowering the value can shorten the rescan time and boot time. However, the time to rescan storage devices might depend on other factors, including the type of storage system and the load on the storage system.

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

Procedure

1 In the vSphere Client inventory panel, select the host, click the **Configuration** tab, and click **Advanced Settings** under Software.

2 Select **Disk**.

3 Scroll down to **Disk.MaxLUN**.

4 Change the existing value to the value of your choice, and click **OK**.

The value you enter specifies the LUN ID after the last one you want to discover.

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

Working with Datastores

Datastores are logical containers, analogous to file systems, that hide specifics of each storage device and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

You use the vSphere Client to access different types of storage devices that your ESXi host discovers and to deploy datastores on them.

Depending on the type of storage you use, datastores can be backed by the following file system formats:

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

After creating datastores, you can organize them in different ways. For example, you can group them into folders according to business practices. This allows you to assign the same permissions and alarms on the datastores in the group at one time.

You can also add datastores to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create a datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the *vSphere Resource Management* documentation.

Create a VMFS Datastore in the vSphere Client

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Before creating datastores, you must install and configure any adapters that your storage requires. Rescan the adapters to discover newly added storage devices.

Procedure

1 Log in to the vSphere Client and select the host from the Inventory panel.

2 Click the **Configuration** tab and click **Storage** in the Hardware panel.

3 Click **Datastores** and click **Add Storage**.

4 Select the **Disk/LUN** storage type and click **Next**.

5 Select a device to use for your datastore and click **Next**.

Important Select the device that does not have a datastore name displayed in the VMFS Label column. If a name is present, the device contains a copy of an existing VMFS datastore.

6 Select the **File System Version** and click **Next**.

Important If you select VMFS3 you must select the maximum file size under **Formatting**.

7 If the disk is not blank, review the current disk layout in the top panel of the Current Disk Layout page and select a configuration option from the bottom panel.

Option	Description
Use all available partitions	Dedicates the entire disk to a single VMFS datastore. If you select this option, all file systems and data currently stored on this device are destroyed.
Use free space	Deploys a VMFS datastore in the remaining free space of the disk.

If the disk you are formatting is blank, the **Current Disk Layout** page presents the entire disk space for storage configuration.

8 Click **Next**.

9 On the **Properties** page, type a datastore name and click **Next**.

10 If the space specified for storage is excessive for your purposes, you can adjust the capacity values.

   By default, the entire free space on the storage device is available.

11 Click **Next**.

12 In the Ready to Complete page, review the datastore configuration information and click **Finish**.

A datastore on the SCSI-based storage device is created. If you use the vCenter Server system to manage your hosts, the newly created datastore is added to all hosts.

Create NFS Datastore in the vSphere Client

You can use the Add Storage wizard to mount an NFS volume and use it as if it were a VMFS datastore.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1 Log in to the vSphere Client and select the host from the Inventory panel.

2 Click the **Configuration** tab and click **Storage** in the Hardware panel.

3 Click **Datastores** and click **Add Storage**.

4 Select **Network File System** as the storage type and click **Next**.

5 Enter the server name, the mount point folder name, and the datastore name.

   For the server name, you can enter an IP address, a DNS name, or an NFS UUID.

   NOTE When you mount the same NFS volume on different hosts, make sure that the server and folder names are identical across the hosts. If the names do not match exactly, the hosts see the same NFS volume as two different datastores. This might result in a failure of such features as vMotion. An example of such discrepancy could be if you enter `filer` as the server name on one host and `filer.domain.com` on the other.

6 (Optional) Select **Mount NFS read only** if the volume is exported as read only by the NFS server.

7 Click **Next**.

8 In the Network File System Summary page, review the configuration options and click **Finish**.

Managing Duplicate VMFS Datastores

When a storage device contains a VMFS datastore copy, you can mount the datastore with the existing signature or assign a new signature.

Each VMFS datastore created in a storage disk has a unique signature, also called UUID, that is stored in the file system superblock. When the storage disk is replicated or its snapshot is taken on the storage side, the resulting disk copy is identical, byte-for-byte, with the original disk. As a result, if the original storage disk contains a VMFS datastore with UUID X, the disk copy appears to contain an identical VMFS datastore, or a VMFS datastore copy, with exactly the same UUID X.

In addition to LUN snapshotting and replication, the following storage device operations might cause ESXi to mark the existing datastore on the device as a copy of the original datastore:

- LUN ID changes
- SCSI device type changes, for example, from SCSI-2 to SCSI-3

- SPC-2 compliancy enablement

ESXi can detect the VMFS datastore copy and display it in the vSphere Client or the vSphere Web Client. You have an option of mounting the datastore copy with its original UUID or changing the UUID to resignature the datastore.

Whether you chose resignaturing or mounting without resignaturing depends on how the LUNs are masked in the storage environment. If your hosts are able to see both copies of the LUN, then resignaturing is the recommended method. Otherwise, mounting is an option.

Keep Existing Datastore Signature in the vSphere Client

If you do not need to resignature a VMFS datastore copy, you can mount it without changing its signature.

You can keep the signature if, for example, you maintain synchronized copies of virtual machines at a secondary site as part of a disaster recovery plan. In the event of a disaster at the primary site, you mount the datastore copy and power on the virtual machines at the secondary site.

Important You can mount a VMFS datastore copy only if it does not collide with the original VMFS datastore that has the same UUID. To mount the copy, the original VMFS datastore has to be offline.

When you mount the VMFS datastore, ESXi allows both reads and writes to the datastore residing on the LUN copy. The LUN copy must be writable. The datastore mounts are persistent and valid across system reboots.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Before you mount a VMFS datastore, perform a storage rescan on your host so that it updates its view of LUNs presented to it.

Procedure

1. Log in to the vSphere Client and select the server from the inventory panel.
2. Click the **Configuration** tab and click **Storage** in the Hardware panel.
3. Click **Add Storage**.
4. Select the **Disk/LUN** storage type and click **Next**.
5. From the list of LUNs, select the LUN that has a datastore name displayed in the VMFS Label column and click **Next**.

   The name present in the VMFS Label column indicates that the LUN is a copy that contains a copy of an existing VMFS datastore.
6. Under Mount Options, select **Keep Existing Signature**.
7. In the Ready to Complete page, review the datastore configuration information and click **Finish**.

What to do next

If you later want to resignature the mounted datastore, you must unmount it first.

Resignature a VMFS Datastore Copy in the vSphere Client

Use datastore resignaturing if you want to retain the data stored on the VMFS datastore copy.

When resignaturing a VMFS copy, ESXi assigns a new UUID and a new label to the copy, and mounts the copy as a datastore distinct from the original.

The default format of the new label assigned to the datastore is `snap-snapID-oldLabel`, where *snapID* is an integer and *oldLabel* is the label of the original datastore.

When you perform datastore resignaturing, consider the following points:

- Datastore resignaturing is irreversible.
- The LUN copy that contains the VMFS datastore that you resignature is no longer treated as a LUN copy.
- A spanned datastore can be resignatured only if all its extents are online.
- The resignaturing process is crash and fault tolerant. If the process is interrupted, you can resume it later.
- You can mount the new VMFS datastore without a risk of its UUID colliding with UUIDs of any other datastore, such as an ancestor or child in a hierarchy of LUN snapshots.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

To resignature a mounted datastore copy, first unmount it.

Before you resignature a VMFS datastore, perform a storage rescan on your host so that the host updates its view of LUNs presented to it and discovers any LUN copies.

Procedure

1. Log in to the vSphere Client and select the server from the inventory panel.
2. Click the **Configuration** tab and click **Storage** in the Hardware panel.
3. Click **Add Storage**.
4. Select the **Disk/LUN** storage type and click **Next**.
5. From the list of LUNs, select the LUN that has a datastore name displayed in the VMFS Label column and click **Next**.

   The name present in the VMFS Label column indicates that the LUN is a copy that contains a copy of an existing VMFS datastore.
6. Under Mount Options, select **Assign a New Signature** and click **Next**.
7. In the Ready to Complete page, review the datastore configuration information and click **Finish**.

What to do next

After resignaturing, you might have to do the following:

- If the resignatured datastore contains virtual machines, update references to the original VMFS datastore in the virtual machine files, including `.vmx`, `.vmdk`, `.vmsd`, and `.vmsn`.
- To power on virtual machines, register them with vCenter Server.

Upgrading VMFS Datastores

If your datastores were formatted with VMFS2 or VMFS3, you must upgrade the datastores to VMFS5.

When you perform datastore upgrades, consider the following items:

- To upgrade a VMFS2 datastore, you use a two-step process that involves upgrading VMFS2 to VMFS3 first. To access the VMFS2 datastore and perform the VMFS2 to VMFS3 conversion, use an ESX/ESXi 4.x or earlier host.

  After you upgrade your VMFS2 datastore to VMFS3, the datastore becomes available on the ESXi 6.0 host, where you complete the process of upgrading to VMFS5.
- You can perform a VMFS3 to VMFS5 upgrade while the datastore is in use with virtual machines powered on.

- While performing an upgrade, your host preserves all files on the datastore.
- The datastore upgrade is a one-way process. After upgrading your datastore, you cannot revert it back to its previous VMFS format.

An upgraded VMFS5 datastore differs from a newly formatted VMFS5.

Table 24-3. Comparing Upgraded and Newly Formatted VMFS5 Datastores

Characteristics	Upgraded VMFS5	Formatted VMFS5
File block size	1, 2, 4, and 8MB	1MB
Subblock size	64KB	8KB
Partition format	MBR. Conversion to GPT happens only after you expand the datastore to a size larger than 2TB.	GPT
Datastore limits	Retains limits of VMFS3 datastore.	
VMFS locking mechanism	ATS+SCSI	ATS-only (on hardware that supports ATS) ATS+SCSI (on hardware that does not support ATS)

For more information about VMFS locking mechanisms and how to upgrade to ATS-only, see the *vSphere Storage* publication.

Upgrade VMFS2 Datastores to VMFS3

If your datastore was formatted with VMFS2, you must first upgrade it to VMFS3. Because ESXi 5.x hosts cannot access VMFS2 datastores, use a legacy host, ESX/ESXi 4.x or earlier, to access the VMFS2 datastore and perform the VMFS2 to VMFS3 upgrade.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Commit or discard any changes to virtual disks in the VMFS2 datastore that you plan to upgrade.
- Back up the VMFS2 datastore.
- Be sure that no powered on virtual machines are using the VMFS2 datastore.
- Be sure that no other ESXi host is accessing the VMFS2 datastore.
- To upgrade the VMFS2 file system, its file block size must not exceed 8MB.

Procedure

1. Log in to the vSphere Client, and select a host from the inventory panel.
2. Click the **Configuration** tab and click **Storage**.
3. Select the datastore that uses the VMFS2 format.
4. Click **Upgrade to VMFS3**.
5. Perform a rescan on all hosts that see the datastore.

What to do next

After you upgrade your VMFS2 datastore to VMFS3, the datastore becomes available on the ESXi 5.x host. You can now use the ESXi 5.x host to complete the process of upgrading to VMFS5.

Upgrade VMFS3 Datastores to VMFS5 in the vSphere Client

VMFS5 is a new version of the VMware cluster file system that provides performance and scalability improvements.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- If you use a VMFS2 datastore, you must first upgrade it to VMFS3. Follow the instructions in "Upgrade VMFS2 Datastores to VMFS3," on page 327.
- All hosts accessing the datastore must support VMFS5.
- Verify that the volume to be upgraded has at least 2MB of free blocks available and 1 free file descriptor.

Procedure

1. Log in to the vSphere Client, and select a host from the inventory panel.
2. Click the **Configuration** tab and click **Storage**.
3. Select the VMFS3 datastore.
4. Click **Upgrade to VMFS5**.

   A warning message about host version support appears.
5. Click **OK** to start the upgrade.

   The task `Upgrade VMFS` appears in the **Recent Tasks** list.
6. Perform a rescan on all hosts that are associated with the datastore.

Increase VMFS Datastore Capacity in the vSphere Client

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

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

- Add a new extent. An extent is a partition on a storage device. You can add up to 32 extents of the same storage type to an existing VMFS datastore. The spanned VMFS datastore can use any or all of its extents at any time. It does not need to fill up a particular extent before using the next one.
- Grow an extent in an existing VMFS datastore, so that it fills the available adjacent capacity. Only extents with free space immediately after them are expandable.

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

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

Procedure

1. Log in to the vSphere Client and select a host from the Inventory panel.
2. Click the **Configuration** tab and click **Storage**.
3. From the Datastores view, select the datastore to increase and click **Properties**.

4 Click **Increase**.

5 Select a device from the list of storage devices and click **Next**.

Option	Description
To add a new extent	Select the device for which the Expandable column reads NO.
To expand an existing extent	Select the device for which the Expandable column reads YES

6 Review the **Current Disk Layout** to see the available configurations and click **Next**.

7 Select a configuration option from the bottom panel.

Depending on the current layout of the disk and on your previous selections, the options you see might vary.

Option	Description
Use free space to add new extent	Adds the free space on this disk as a new extent.
Use free space to expand existing extent	Expands an existing extent to a required capacity.
Use free space	Deploys an extent in the remaining free space of the disk. This option is available only when you are adding an extent.
Use all available partitions	Dedicates the entire disk to a single extent. This option is available only when you are adding an extent and when the disk you are formatting is not blank. The disk is reformatted, and the datastores and any data that it contains are erased.

8 Set the capacity for the extent.

The minimum extent size is 1.3GB. By default, the entire free space on the storage device is available.

9 Click **Next**.

10 Review the proposed layout and the new configuration of your datastore, and click **Finish**.

What to do next

After you grow an extent in a shared VMFS datastore, refresh the datastore on each host that can access this datastore, so that the vSphere Client can display the correct datastore capacity for all hosts.

Rename VMFS or NFS Datastores in the vSphere Client

You can change the name of an existing datastore.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Display the datastores.

2 Right-click the datastore to rename and select **Rename**.

3 Type a new datastore name.

If you use the vCenter Server system to manage your hosts, the new name appears on all hosts that have access to the datastore.

Group VMFS or NFS Datastores in the vSphere Client

If you use the vCenter Server system to manage your hosts, group datastores into folders. This allows you to organize your datastores according to business practices and to assign the same permissions and alarms on the datastores in the group at one time.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client.

2 If necessary, create the datastores.

3 In the Inventory panel, choose **Datastores**.

4 Select the datacenter containing the datastores to group.

5 In the shortcut menu, click the **New Folder** icon.

6 Give the folder a descriptive name.

7 Click and drag each datastore onto the folder.

Delete VMFS Datastores in the vSphere Client

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

Note The datastore delete operation permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

Prerequisites

- Open a vSphere Client connection to a vCenter Server.
- Remove all virtual machines from the datastore.
- Make sure that no other host is accessing the datastore.

Procedure

1 Display the datastores.

2 Right-click the datastore to delete and click **Delete**.

3 Confirm that you want to delete the datastore.

Create a Diagnostic Partition in the vSphere Client

You can create a diagnostic partition for your host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select the host from the Inventory panel.

2 Click the **Configuration** tab and click **Storage** in the Hardware panel.

3 Click **Datastores** and click **Add Storage**.

4 Select **Diagnostic** and click **Next**.

If you do not see **Diagnostic** as an option, the host already has a diagnostic partition.

5 Specify the type of diagnostic partition.

Option	Description
Private Local	Creates the diagnostic partition on a local disk. This partition stores fault information only for your host.
Private SAN Storage	Creates the diagnostic partition on a non-shared SAN LUN. This partition stores fault information only for your host.
Shared SAN Storage	Creates the diagnostic partition on a shared SAN LUN. This partition is accessed by multiple hosts and can store fault information for more than one host.

6 Click **Next**.

7 Select the device to use for the diagnostic partition and click **Next**.

8 Review the partition configuration information and click **Finish**.

Turn off Storage Filters

When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Before making any changes to the device filters, consult with the VMware support team. You can turn off the filters only if you have other methods to prevent device corruption.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select **Administration > vCenter Server Settings**.

2 In the settings list, select **Advanced Settings**.

3 In the **Key** text box, type a key.

Key	Filter Name
config.vpxd.filter.vmfsFilter	VMFS Filter
config.vpxd.filter.rdmFilter	RDM Filter
config.vpxd.filter.SameHostAndTransportsFilter	Same Host and Transports Filter
config.vpxd.filter.hostRescanFilter	Host Rescan Filter NOTE If you turn off the Host Rescan Filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.

4 In the **Value** text box, type `False` for the specified key.

5 Click **Add**.

6 Click **OK**.

You are not required to restart the vCenter Server system.

Raw Device Mapping

Raw device mapping (RDM) provides a mechanism for a virtual machine to have direct access to a LUN on the physical storage subsystem (Fibre Channel or iSCSI only).

The following topics contain information about RDMs and provide instructions on how to create and manage RDMs.

Create Virtual Machines with RDMs

When you give your virtual machine direct access to a raw SAN LUN, you create a mapping file (RDM) that resides on a VMFS datastore and points to the LUN. Although the mapping file has the same `.vmdk` extension as a regular virtual disk file, the RDM file contains only mapping information. The actual virtual disk data is stored directly on the LUN.

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Follow all steps required to create a custom virtual machine.

2 In the Select a Disk page, select **Raw Device Mapping**, and click **Next**.

3 From the list of SAN disks or LUNs, select a raw LUN for your virtual machine to access directly.

4 Select a datastore for the RDM mapping file.

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

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

5 Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, powered on virtual machines that use RDMs configured for physical compatibility cannot be migrated if the migration involves copying the disk. Such virtual machines cannot be cloned or cloned to a template either.
Virtual	Allows the RDM to behave as if it were a virtual disk, so you can use such features as snapshotting, cloning, and so on.

6 Select a virtual device node.

7 If you select Independent mode, choose one of the following.

Option	Description
Persistent	Changes are immediately and permanently written to the disk.
Nonpersistent	Changes to the disk are discarded when you power off or revert to the snapshot.

8 Click **Next**.

9 In the Ready to Complete New Virtual Machine page, review your selections.

10 Click **Finish** to complete your virtual machine.

Manage Paths for a Mapped Raw LUN

You can manage paths for mapped raw LUNs.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Log in as administrator or as the owner of the virtual machine to which the mapped disk belongs.

2 Select the virtual machine from the Inventory panel.

3 On the **Summary** tab, click **Edit Settings**.

4 On the **Hardware** tab, select **Hard Disk**, then click **Manage Paths**.

5 Use the Manage Paths dialog box to enable or disable your paths, set multipathing policy, and specify the preferred path.

For information on managing paths, see "Understanding Multipathing and Failover," on page 333.

Understanding Multipathing and Failover

To maintain a constant connection between a host and its storage, ESXi supports multipathing. Multipathing is a technique that lets you use more than one physical path that transfers data between the host and an external storage device.

In case of a failure of any element in the SAN network, such as an adapter, switch, or cable, ESXi can switch to another physical path, which does not use the failed component. This process of path switching to avoid failed components is known as path failover.

In addition to path failover, multipathing provides load balancing. Load balancing is the process of distributing I/O loads across multiple physical paths. Load balancing reduces or removes potential bottlenecks.

NOTE Virtual machine I/O might be delayed for up to sixty seconds while path failover takes place. These delays allow the SAN to stabilize its configuration after topology changes. In general, the I/O delays might be longer on active-passive arrays and shorter on active-active arrays.

Path Scanning and Claiming

When you start your ESXi host or rescan your storage adapter, the host discovers all physical paths to storage devices available to the host. Based on a set of claim rules, the host determines which multipathing plug-in (MPP) should claim the paths to a particular device and become responsible for managing the multipathing support for the device.

By default, the host performs a periodic path evaluation every 5 minutes causing any unclaimed paths to be claimed by the appropriate MPP.

The claim rules are numbered. For each physical path, the host runs through the claim rules starting with the lowest number first. The attributes of the physical path are compared to the path specification in the claim rule. If there is a match, the host assigns the MPP specified in the claim rule to manage the physical path. This continues until all physical paths are claimed by corresponding MPPs, either third-party multipathing plug-ins or the native multipathing plug-in (NMP).

For the paths managed by the NMP module, a second set of claim rules is applied. These rules determine which Storage Array Type Plug-In (SATP) should be used to manage the paths for a specific array type, and which Path Selection Plug-In (PSP) is to be used for each storage device.

Use the vSphere Client to view which SATP and PSP the host is using for a specific storage device and the status of all available paths for this storage device. If needed, you can change the default VMware PSP using the client. To change the default SATP, you need to modify claim rules using the vSphere CLI.

You can find some information about modifying claim rules in the *vSphere Storage* documentation.

For more information about the commands available to manage PSA, see *Getting Started with vSphere Command-Line Interfaces*.

For a complete list of storage arrays and corresponding SATPs and PSPs, see the SAN Array Model Reference section of the *vSphere Compatibility Guide*.

View Datastore Paths in the vSphere Client

Use the vSphere Client to review the paths that connect to storage devices the datastores are deployed on.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage** in the Hardware panel.

3 Click **Datastores** under View.

4 From the list of configured datastores, select the datastore whose paths you want to view, and click **Properties**.

5 Under Extents, select the storage device whose paths you want to view and click **Manage Paths**.

6 In the Paths panel, select the path to view.

   The panel underneath displays the path's name. The name includes parameters describing the path: adapter ID, target ID, and device ID.

7 (Optional) To extract the path's parameters, right-click the path and select **Copy path to clipboard**.

View Storage Device Paths in the vSphere Client

Use the vSphere Client to view which SATP and PSP the host uses for a specific storage device and the status of all available paths for this storage device.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Log in to the vSphere Client and select a server from the inventory panel.

2 Click the **Configuration** tab and click **Storage** in the Hardware panel.

3 Click **Devices** under View.

4 Select the storage device whose paths you want to view and click **Manage Paths**.

5 In the Paths panel, select the path to view.

   The panel underneath displays the path's name. The name includes parameters describing the path: adapter ID, target ID, and device ID.

6 (Optional) To extract the path's parameters, right-click the path and select **Copy path to clipboard**.

Change the Path Selection Policy in the vSphere Client

Generally, you do not have to change the default multipathing settings your host uses for a specific storage device. However, if you want to make any changes, you can use the Manage Paths dialog box to modify a path selection policy and specify the preferred path for the Fixed policy.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Open the Manage Paths dialog box either from the Datastores or Devices view.

2 Select a path selection policy.

By default, VMware supports the following path selection policies. If you have a third-party PSP installed on your host, its policy also appears on the list.

- Fixed (VMware)
- Most Recently Used (VMware)
- Round Robin (VMware)

3 For the fixed policy, specify the preferred path by right-clicking the path you want to assign as the preferred path, and selecting **Preferred**.

4 Click **OK** to save your settings and exit the dialog box.

Disable Paths in the vSphere Client

You can temporarily disable paths for maintenance or other reasons. You can do so using the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Open the Manage Paths dialog box either from the Datastores or Devices view.

2 In the Paths panel, right-click the path to disable, and select **Disable**.

3 Click **OK** to save your settings and exit the dialog box.

You can also disable a path from the adapter's Paths view by right-clicking the path in the list and selecting **Disable**.

Storage Hardware Acceleration

The hardware acceleration functionality enables the ESXi host to integrate with compliant storage arrays and offload specific virtual machine and storage management operations to storage hardware. With the storage hardware assistance, your host performs these operations faster and consumes less CPU, memory, and storage fabric bandwidth.

The hardware acceleration is supported by block storage devices, Fibre Channel and iSCSI, and NAS devices.

For additional details, see the VMware knowledge base article at http://kb.vmware.com/kb/1021976.

Disable Hardware Acceleration for Block Storage Devices

On your host, the hardware acceleration for block storage devices is enabled by default. You can use the vSphere Client advanced settings to disable the hardware acceleration operations.

As with any advanced settings, before you disable the hardware acceleration, consult with the VMware support team.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory panel, select the host.

2 Click the **Configuration** tab, and click **Advanced Settings** under **Software.**

3 Change the value for any of the options to 0 (disabled):

- VMFS3.HardwareAcceleratedLocking
- DataMover.HardwareAcceleratedMove
- DataMover.HardwareAcceleratedInit

Storage Thin Provisioning

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

Thin provisioning is a method that optimizes storage utilization by allocating storage space in a flexible on-demand manner. Thin provisioning contrasts with the traditional model, called thick provisioning. With thick provisioning, large amount of storage space is provided in advance in anticipation of future storage needs. However, the space might remain unused causing underutilization of storage capacity.

The VMware thin provisioning features help you eliminate storage underutilization problems at the datastore and storage array level.

Create Thin Provisioned Virtual Disks

When you need to save storage space, you can create a virtual disk in thin provisioned format. The thin provisioned virtual disk starts small and grows as more disk space is required.

This procedure assumes that you are creating a typical or custom virtual machine using the New Virtual Machine wizard.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

You can create thin disks only on the datastores that support disk-level thin provisioning.

Procedure

◆ In the Create a Disk dialog box, select **Thin Provision**.

A virtual disk in thin format is created.

What to do next

If you created a virtual disk in the thin format, you can later inflate it to its full size.

View Virtual Machine Storage Resources

You can view how datastore storage space is allocated for your virtual machines.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Select the virtual machine in the inventory.

2 Click the **Summary** tab.

3 Review the space allocation information in the Resources section.

- Provisioned Storage – Shows datastore space allocated to the virtual machine. The entire space might not be used by the virtual machine if it has disks in thin provisioned format. Other virtual machines can occupy any unused space.
- Not-shared Storage – Shows datastore space occupied by the virtual machine and not shared with any other virtual machines.
- Used Storage – Shows datastore space actually occupied by virtual machine files, including configuration and log files, snapshots, virtual disks, and so on. When the virtual machine is running, the used storage space also includes swap files.

Determine the Disk Format of a Virtual Machine

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Select the virtual machine in the inventory.

2 Click **Edit Settings** to display the Virtual Machine Properties dialog box.

3 Click the **Hardware** tab and select the appropriate hard disk in the Hardware list.

The Disk Provisioning section on the right shows the type of your virtual disk.

4 Click **OK**.

What to do next

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

Inflate Thin Virtual Disks

If you created a virtual disk in the thin provision format, you can inflate it to its full size.

This procedure converts a thin disk to a virtual disk in thick provision format.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Select the virtual machine in the inventory.

2 Click the **Summary** tab and, under Resources, double-click the datastore for the virtual machine to open the Datastore Browser dialog box.

3 Click the virtual machine folder to find the virtual disk file you want to convert. The file has the `.vmdk` extension.

4 Right-click the virtual disk file and select **Inflate**.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Using Storage Vendor Providers

When using vendor provider components, the vCenter Server can integrate with external storage, both block storage and NFS, so that you can gain a better insight into resources and obtain comprehensive and meaningful storage data.

The vendor provider is a software plug-in developed by a third party through the Storage APIs - Storage Awareness. The vendor provider component is typically installed on the storage array side and acts as a server in the vSphere environment. The vCenter Server uses vendor providers to retrieve information about storage topology, capabilities, and status.

For information about whether your storage supports the vendor provider plug-ins, contact your storage vendor.

If your storage supports vendor providers, use the **Storage Providers** menu option in the vSphere Client or the vSphere Web Client to register and manage each vendor provider component.

Register Vendor Providers in the vSphere Client

To establish a connection between the vCenter Server and a vendor provider, you must register the vendor provider.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Verify that the vendor provider component is installed on the storage side and obtain its credentials from your storage administrator.

Procedure

1 Select **View > Administration > Storage Providers**.

2 Click **Add**.

3 In the **Add Vendor Provider** dialog box, type connection information for the vendor provider, including the name, URL, and credentials.

4 (Optional) To direct the vCenter Server to the vendor provider certificate, select the **Use Vendor Provider Certificate** option and specify the certificate's location.

   If you do not select this option, the vSphere Client displays a thumbprint of the certificate. You can check the thumbprint and approve it.

5 Click **OK** to complete the registration.

The vCenter Server has registered the vendor provider and established a secure SSL connection with it.

View Vendor Provider Information

After you register a vendor provider component with the vCenter Server, the vendor provider appears on the vendor providers list in the vSphere Client.

View general vendor provider information and details for each vendor component.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select **View > Administration > Storage Providers**.

2 In the Vendor Providers list, view the vendor provider components registered with the vCenter Server.

The list shows general vendor information including the name, URL, and the time of the last view refresh.

3 To display additional details, select a specific vendor provider from the list.

The details include storage array vendors and array models that the vendor provider supports.

NOTE A single vendor provider can support storage arrays from multiple different vendors.

Unregister Vendor Providers

Unregister vendor providers that you do not need.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select **View > Administration > Storage Providers**.

2 From the list of vendor providers, select the one you want to unregister and click **Remove**.

The vCenter Server terminates the connection and removes the vendor provider from its configuration.

Update Vendor Providers

The vCenter Server periodically updates storage data in its database. The updates are partial and reflect only those storage changes that storage providers communicate to the vCenter Server. When needed, you can perform a full database synchronisation for the selected storage provider.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select **View > Administration > Storage Providers**.

2 From the list, select the vendor provider that you want to synchronise with and click **Sync**.

The vSphere Client updates the storage data for the provider.

Resource Management for Single Hosts

25

When you connect the vSphere Client directly to a host, you have access to a limited number of resource management settings, including hyperthreading settings, power management configuration, and swapfile properties.

This chapter includes the following topics:

- "Configuring Resource Allocation Settings," on page 341
- "Administering CPU Resources," on page 342
- "Administering Memory Resources," on page 345
- "Managing Storage I/O Resources," on page 349
- "Managing Resource Pools," on page 352
- "Using DRS Clusters to Manage Resources," on page 356
- "Creating a Datastore Cluster," on page 368
- "Using Datastore Clusters to Manage Storage Resources," on page 371
- "Using NUMA Systems with ESXi," on page 379
- "Advanced Attributes," on page 381

Configuring Resource Allocation Settings

When available resource capacity does not meet the demands of the resource consumers (and virtualization overhead), administrators might need to customize the amount of resources that are allocated to virtual machines or to the resource pools in which they reside.

Use the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine. In particular, administrators have several options for allocating resources.

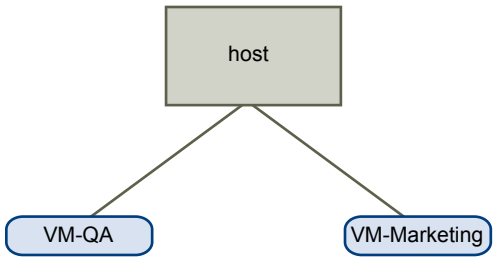
- Reserve the physical resources of the host or cluster.
- Set an upper bound on the resources that can be allocated to a virtual machine.
- Guarantee that a particular virtual machine is always allocated a higher percentage of the physical resources than other virtual machines.

Changing Resource Allocation Settings—Example

The following example illustrates how you can change resource allocation settings to improve virtual machine performance.

Assume that on an ESXi host, you have created two new virtual machines—one each for your QA (VM-QA) and Marketing (VM-Marketing) departments.

Figure 25-1. Single Host with Two Virtual Machines



In the following example, assume that VM-QA is memory intensive and accordingly you want to change the resource allocation settings for the two virtual machines to:

- Specify that, when system memory is overcommitted, VM-QA can use twice as much memory and CPU as the Marketing virtual machine. Set the memory shares and CPU shares for VM-QA to **High** and for VM-Marketing set them to **Normal**.
- Ensure that the Marketing virtual machine has a certain amount of guaranteed CPU resources. You can do so using a reservation setting.

Procedure

1 Start the vSphere Client and connect to a vCenter Server system.

2 Right-click **VM-QA**, the virtual machine for which you want to change shares, and select **Edit Settings**.

3 Select the **Resources** tab, and in the CPU panel, select **High** from the **Shares** drop-down menu.

4 In the Memory panel, select **High** from the **Shares** drop-down menu.

5 Click **OK**.

6 Right-click the marketing virtual machine (**VM-Marketing**) and select **Edit Settings**.

7 In the CPU panel, change the **Reservation** value to the desired number.

8 Click **OK**.

If you select the cluster's **Resource Allocation** tab and click **CPU**, you should see that shares for **VM-QA** are twice that of the other virtual machine. Also, because the virtual machines have not been powered on, the **Reservation Used** fields have not changed.

Administering CPU Resources

You can configure virtual machines with one or more virtual processors, each with its own set of registers and control structures.

When a virtual machine is scheduled, its virtual processors are scheduled to run on physical processors. The VMkernel Resource Manager schedules the virtual CPUs on physical CPUs, thereby managing the virtual machine's access to physical CPU resources. ESXi supports virtual machines with up to 128 virtual CPUs.

View Processor Information

You can access information about current CPU configuration through the vSphere Client or using the vSphere SDK.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host and click the **Configuration** tab.

2 Select **Processors**.

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

   NOTE In hyperthreaded systems, each hardware thread is a logical processor. For example, a dual-core processor with hyperthreading enabled has two cores and four logical processors.

3 (Optional) You can also disable or enable hyperthreading by clicking **Properties**.

Enable Hyperthreading

To enable hyperthreading, you must first enable it in your system's BIOS settings and then turn it on in the vSphere Client. Hyperthreading is enabled by default.

Consult your system documentation to determine whether your CPU supports hyperthreading.

Prerequisites

- Ensure that your system supports hyperthreading technology.
- Enable hyperthreading in the system BIOS. Some manufacturers label this option **Logical Processor**, while others call it **Enable Hyperthreading**.
- Open a vSphere Client connection to a vCenter Server.

Procedure

◆ Tturn on hyperthreading for the ESXi host.

   a In the vSphere Client, select the host and click the **Configuration** tab.

   b Select **Processors** and click **Properties**.

   c In the dialog box, you can view hyperthreading status and turn hyperthreading off or on (default).

Hyperthreading is enabled.

Set Hyperthreading Sharing Options for a Virtual Machine

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

Two virtual CPUs share a core if they are running on logical CPUs of the core at the same time. You can set this for individual virtual machines.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory panel, right-click the virtual machine and select **Edit Settings**.

2 Click the **Resources** tab, and click **Advanced CPU**.

3 Select a hyperthreading mode for this virtual machine from the **Mode** drop-down menu.

Assign a Virtual Machine to a Specific Processor

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

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory panel, select a virtual machine and select **Edit Settings**.

2 Select the **Resources** tab and select **Advanced CPU**.

3 Click the **Run on processor(s)** button.

4 Select the processors where you want the virtual machine to run and click **OK**.

Select a CPU Power Management Policy

You set the CPU power management policy for a host using the vSphere Client.

Prerequisites

ESX/ESXi supports the Enhanced Intel SpeedStep and Enhanced AMD PowerNow! CPU power management technologies. For the VMkernel to take advantage of the power management capabilities provided by these technologies, you must enable power management, sometimes called Demand-Based Switching (DBS), in the BIOS.

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory panel, select a host and click the **Configuration** tab.

2 Under Hardware, select **Power Management** and select **Properties**.

3 Select a power management policy for the host and click **OK**.

The policy selection is saved in the host configuration and can be used again at boot time. You can change it at any time, and it does not require a server reboot.

Configure Custom Policy Parameters for Host Power Management

When you use the Custom policy for host power management, ESXi bases its power management policy on the values of several advanced configuration parameters.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Select **Custom** for the power management policy, as described in "Select a CPU Power Management Policy," on page 344.

Procedure

1 In the vSphere Client inventory, select the host and click the **Configuration** tab.

2 Under Software, select **Advanced Settings**.

3 Click **Power** in the left pane.

4 In the right pane, you can edit the power management parameters that affect the Custom policy.

Power management parameters that affect the Custom policy have descriptions that begin with **In Custom policy**. All other power parameters affect all power management policies.

NOTE The default values of power management parameters match the Balanced policy.

Parameter	Description
Power.UsePStates	Use ACPI P-states to save power when the processor is busy.
Power.MaxCpuLoad	Use P-states to save power on a CPU only when the CPU is busy for less than the given percentage of real time.
Power.MinFreqPct	Do not use any P-states slower than the given percentage of full CPU speed.
Power.UseStallCtr	Use a deeper P-state when the processor is frequently stalled waiting for events such as cache misses.
Power.TimerHz	Controls how many times per second ESXi reevaluates which P-state each CPU should be in.
Power.UseCStates	Use deep ACPI C-states (C2 or below) when the processor is idle.
Power.CStateMaxLatency	Do not use C-states whose latency is greater than this value.
Power.CStateResidencyCoef	When a CPU becomes idle, choose the deepest C-state whose latency multiplied by this value is less than the host's prediction of how long the CPU will remain idle. Larger values make ESXi more conservative about using deep C-states, while smaller values are more aggressive.
Power.CStatePredictionCoef	A parameter in the ESXi algorithm for predicting how long a CPU that becomes idle will remain idle. Changing this value is not recommended.
Power.PerfBias	Performance Energy Bias Hint (Intel-only). Sets an MSR on Intel processors to an Intel-recommended value. Intel recommends 0 for high performance, 6 for balanced, and 15 for low power. Other values are undefined.

Administering Memory Resources

Using the vSphere Client you can view information about and make changes to memory allocation settings. To administer your memory resources effectively, you must also be familiar with memory overhead, idle memory tax, and how ESXi hosts reclaim memory.

When administering memory resources, you can specify memory allocation. If you do not customize memory allocation, the ESXi host uses defaults that work well in most situations.

You can specify memory allocation in several ways.

- Use the attributes and special features available through the vSphere Client. The vSphere Client user interface allows you to connect to the ESXi host or vCenter Server system.
- Use advanced settings.
- Use the vSphere SDK for scripted memory allocation.

Enable Host-Local Swap for a DRS Cluster

Host-local swap allows you to specify a datastore stored locally on the host as the swap file location. You can enable host-local swap for a DRS cluster.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane of the cluster Settings dialog box, click **Swapfile Location**.

3 Select the **Store the swapfile in the datastore specified by the host** option and click **OK**.

4 In the vSphere Client inventory, select one of the hosts in the cluster and click the **Configuration** tab.

5 Under Software, select **Virtual Machine Swapfile Location**.

6 Select the local datastore to use and click **OK**.

7 Repeat Step 4 through Step 6 for each host in the cluster.

Host-local swap is now enabled for the DRS cluster.

Enable Host-Local Swap for a Standalone Host

Host-local swap allows you to specify a datastore stored locally on the host as the swap file location. You can enable host-local swap for a standalone host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration**.

3 Under Software, select **Virtual Machine Swapfile Location**. and click **Edit**.

4 Select **Store the swapfile in the swapfile datastore**.

5 Select a local datastore from the list and click **OK**.

Host-local swap is now enabled for the standalone host.

Configure Virtual Machine Swapfile Properties for the Host

Configure a swapfile location for the host to determine the default location for virtual machine swapfiles.

By default, swapfiles for a virtual machine are located on a VMFS3 datastore in the folder that contains the other virtual machine files. However, you can configure your host to place virtual machine swapfiles on an alternative datastore.

You can use this option to place virtual machine swapfiles on lower-cost or higher-performance storage. You can also override this host-level setting for individual virtual machines.

Setting an alternative swapfile location might cause migrations with vMotion to complete more slowly. For best vMotion performance, store virtual machine swapfiles in the same directory as the virtual machine.

If vCenter Server manages your host, you cannot change the swapfile location if you connect directly to the host by using the vSphere Client. You must connect the vSphere Client to the vCenter Server system.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Host machine.Configuration.Storage partition configuration**

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 Click the **Virtual Machine Swapfile Location** link.

The **Configuration** tab displays the selected swapfile location. If configuration of the swapfile location is not supported on the selected host, the tab indicates that the feature is not supported.

If the host is part of a cluster, and the cluster settings specify that swapfiles are to be stored in the same directory as the virtual machine, you cannot edit the swapfile location from the host configuration tab. To change the swapfile location for such a host, use the Cluster Settings dialog box.

4 Click **Edit**.

5 Select either **Store the swapfile in the same directory as the virtual machine** or **Store the swapfile in a swapfile datastore selected below**.

If you select **Store the swapfile in a swapfile datastore selected below**, select a datastore from the list.

6 Click **OK**.

The virtual machine swapfile is stored in the location you selected.

Configure a Virtual Machine Swapfile Location for a Cluster

By default, swapfiles for a virtual machine are located on a VMFS datastore in the folder that contains the other virtual machine files. However, you can instead configure the hosts in your cluster to place virtual machine swapfiles on an alternative datastore of your choice.

You might choose to configure an alternative swapfile location to place virtual machine swapfiles on either lower-cost or higher-performance storage, depending on your needs.

Note Setting an alternative swapfile location might cause migrations with vMotion to complete more slowly. For best vMotion performance, store virtual machine swapfiles in the same directory as the virtual machine.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Before you configure a virtual machine swapfile location for a cluster, you must configure the virtual machine swapfile locations for the hosts in the cluster as described in "Configure Virtual Machine Swapfile Properties for the Host," on page 346.

Procedure

1 Display the cluster in the inventory.

2 Right-click the cluster and select **Edit Settings**.

3 In the settings list, select **Swapfile Location**.

4 Under Swapfile Policy for Virtual Machines, select where to store the virtual machine swapfile.

Option	Description
Store the swapfile in the same directory as the virtual machine	Stores the swapfile in the same directory as the virtual machine configuration file.
Store the swapfile in the datastore specified by the host	Stores the swapfile in the location specified in the host configuration. If the swapfile cannot be stored on the datastore that the host specifies, the swapfile is stored in the same folder as the virtual machine.

5 Click **OK**.

Delete Swap Files

If a host fails, and that host had running virtual machines that were using swap files, those swap files continue to exist and consume many gigabytes of disk space. You can delete the swap files to eliminate this problem.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system or an ESXi host.

Procedure

1 Restart the virtual machine that was on the host that failed.

2 Stop the virtual machine.

The swap file for the virtual machine is deleted.

Configure the Host Cache

You can change the percentage of space allocated for host cache or disable the host's ability to swap to host cache.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

You must have an SSD-backed datastore in your inventory.

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, click **Host Cache Configuration**.

4 Select the datastore in the list and click **Properties**.

5 Select a size for the host cache allocation on the drive.

6 To disable the ability for the host to swap to host cache on a per-datastore basis, deselect the **Allocate space for host cache** check box.

7 Click **OK**.

Enable or Disable the Memory Compression Cache

Memory compression is enabled by default. You can use the Advanced Settings dialog box in the vSphere Client to enable or disable memory compression for a host.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, select **Advanced Settings**.

4 In the left pane, select **Mem** and locate Mem.MemZipEnable.

5 Enter 1 to enable or enter 0 to disable the memory compression cache.

6 Click **OK**.

Set the Maximum Size of the Memory Compression Cache

You can set the maximum size of the memory compression cache for the host's virtual machines.

You set the size of the compression cache as a percentage of the memory size of the virtual machine. For example, if you enter 20 and a virtual machine's memory size is 1000 MB, ESXi can use up to 200MB of host memory to store the compressed pages of the virtual machine.

If you do not set the size of the compression cache, ESXi uses the default value of 10 percent.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, select **Advanced Settings**.

4 In the left pane, select **Mem** and locate Mem.MemZipMaxPct.

   The value of this attribute determines the maximum size of the compression cache for the virtual machine.

5 Enter the maximum size for the compression cache.

   The value is a percentage of the size of the virtual machine and must be between 5 and 100 percent.

6 Click **OK**.

Managing Storage I/O Resources

vSphere Storage I/O Control allows cluster-wide storage I/O prioritization, which allows better workload consolidation and helps reduce extra costs associated with over provisioning.

Storage I/O Control extends the constructs of shares and limits to handle storage I/O resources. You can control the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion, which ensures that more important virtual machines get preference over less important virtual machines for I/O resource allocation.

When you enable Storage I/O Control on a datastore, ESXi begins to monitor the device latency that hosts observe when communicating with that datastore. When device latency exceeds a threshold, the datastore is considered to be congested and each virtual machine that accesses that datastore is allocated I/O resources in proportion to their shares. You set shares per virtual machine. You can adjust the number for each based on need.

Configuring Storage I/O Control is a two-step process:

1 Enable Storage I/O Control for the datastore.

2 Set the number of storage I/O shares and upper limit of I/O operations per second (IOPS) allowed for each virtual machine.

By default, all virtual machine shares are set to Normal (1000) with unlimited IOPS.

NOTE Storage I/O Control is enabled by default on Storage DRS-enabled datastore clusters.

Storage I/O Control Resource Shares and Limits

You allocate the number of storage I/O shares and upper limit of I/O operations per second (IOPS) allowed for each virtual machine. When storage I/O congestion is detected for a datastore, the I/O workloads of the virtual machines accessing that datastore are adjusted according to the proportion of virtual machine shares each virtual machine has.

Storage I/O shares are similar to those used for memory and CPU resource allocation, which are described in the *vSphere Resource Management* publication. These shares represent the relative importance of a virtual machine with regard to the distribution of storage I/O resources. Under resource contention, virtual machines with higher share values have greater access to the storage array, which typically results in higher throughput and lower latency.

When you allocate storage I/O resources, you can limit the IOPS that are allowed for a virtual machine. By default, these are unlimited. If a virtual machine has more than one virtual disk, you must set the limit on all of its virtual disks. Otherwise, the limit will not be enforced for the virtual machine. In this case, the limit on the virtual machine is the aggregation of the limits for all virtual disks.

The benefits and drawbacks of setting resource limits are described in the *vSphere Resource Management* publication. If the limit you want to set for a virtual machine is in terms of MB per second instead of IOPS, you can convert MB per second into IOPS based on the typical I/O size for that virtual machine. For example, to restrict a backup application with 64KB IOs to 10MB per second, set a limit of 160 IOPS.

View Storage I/O Control Shares and Limits

You can view the shares and limits for all virtual machines running on a datastore. Viewing this information allows you to compare the settings of all virtual machines that are accessing the datastore, regardless of the cluster in which they are running.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the datastore in the vSphere Client inventory.

2 Click the **Virtual Machines** tab.

   The tab displays each virtual machine running on the datastore and the associated shares value, IOPS limit, and percentage of datastore shares.

Monitor Storage I/O Control Shares

Use the datastore **Performance** tab to monitor how Storage I/O Control handles the I/O workloads of the virtual machines accessing a datastore based on their shares.

Datastore performance charts allow you to monitor the following information:

- Average latency and aggregated IOPS on the datastore
- Latency among hosts
- Queue depth among hosts
- Read/write IOPS among hosts
- Read/write latency among virtual machine disks
- Read/write IOPS among virtual machine disks

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the datastore in the vSphere Client inventory and click the **Performance** tab.

2 From the **View** drop-down menu, select **Performance**.

For more information, see the *vSphere Monitoring and Performance* documentation.

Set Storage I/O Control Resource Shares and Limits

Allocate storage I/O resources to virtual machines based on importance by assigning a relative amount of shares to the virtual machine.

Unless virtual machine workloads are very similar, shares do not necessarily dictate allocation in terms of I/O operations or megabytes per second. Higher shares allow a virtual machine to keep more concurrent I/O operations pending at the storage device or datastore compared to a virtual machine with lower shares. Two virtual machines might experience different throughput based on their workloads.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a virtual machine in the vSphere Client inventory.

2 Click the **Summary** tab and click **Edit Settings**.

3 Click the **Resources** tab and select **Disk**.

4 Select a virtual hard disk from the list.

5 Click the **Shares** column to select the relative amount of shares to allocate to the virtual machine (Low, Normal, or High).

You can select **Custom** to enter a user-defined shares value.

6 Click the **Limit - IOPS** column and enter the upper limit of storage resources to allocate to the virtual machine.

IOPS are the number of I/O operations per second. By default, IOPS are unlimited. You select Low (500), Normal (1000), or High (2000), or you can select Custom to enter a user-defined number of shares.

7 Click **OK**.

Shares and limits are reflected on the **Resource Allocation** tab for the host and cluster.

Enable Storage I/O Control

When you enable Storage I/O Control, ESXi monitors datastore latency and adjusts the I/O load sent to it, if datastore average latency exceeds the threshold.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory, select a datastore and click the **Configuration** tab.

2 Click **Properties**.

3 Under Storage I/O Control, select the **Enabled** check box.

4 Click **Close**.

On the Datastores tab, the Storage I/O Control column shows that Storage I/O Control is enabled for the datastore.

Set Storage I/O Control Threshold Value

The congestion threshold value for a datastore is the upper limit of latency that is allowed for a datastore before Storage I/O Control begins to assign importance to the virtual machine workloads according to their shares.

You do not need to adjust the threshold setting in most environments.

Caution Storage I/O Control will not function correctly unless all datatores that share the same spindles on the array have the same congestion threshold.

If you change the congestion threshold setting, set the value based on the following considerations.

- A higher value typically results in higher aggregate throughput and weaker isolation. Throttling will not occur unless the overall average latency is higher than the threshold.
- If throughput is more critical than latency, do not set the value too low. For example, for Fibre Channel disks, a value below 20 ms could lower peak disk throughput. A very high value (above 50 ms) might allow very high latency without any significant gain in overall throughput.
- A lower value will result in lower device latency and stronger virtual machine I/O performance isolation. Stronger isolation means that the shares controls are enforced more often. Lower device latency translates into lower I/O latency for the virtual machines with the highest shares, at the cost of higher I/O latency experienced by the virtual machines with fewer shares.
- If latency is more important, a very low value (lower than 20 ms) will result in lower device latency and better isolation among I/Os at the potential cost of a decrease in aggregate datastore throughput.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Verify that Storage I/O Control is enabled.

Procedure

1. In the vSphere Client inventory, select a datastore and click the **Configuration** tab.
2. Click **Properties**.
3. Under Storage I/O Control, select the **Enabled** check box.
4. (Optional) Click **Advanced** to edit the congestion threshold value for the datastore.

   The value must be between 10 ms and 100 ms.
5. (Optional) Click **Reset** to restore the congestion threshold setting to the default value (30 ms).
6. Click **OK** and click **Close**.

Managing Resource Pools

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources.

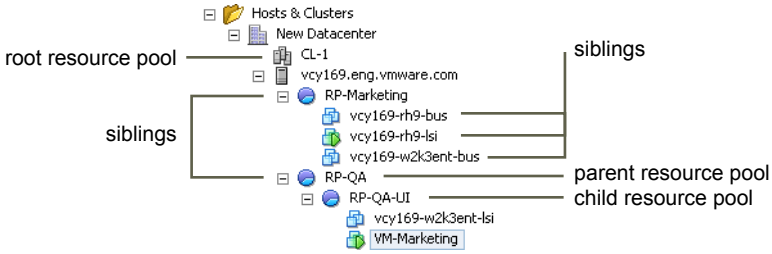
Each standalone host and each DRS cluster has an (invisible) root resource pool that groups the resources of that host or cluster. The root resource pool does not appear because the resources of the host (or cluster) and the root resource pool are always the same.

Users can create child resource pools of the root resource pool or of any user-created child resource pool. Each child resource pool owns some of the parent's resources and can, in turn, have a hierarchy of child resource pools to represent successively smaller units of computational capability.

A resource pool can contain child resource pools, virtual machines, or both. You can create a hierarchy of shared resources. The resource pools at a higher level are called parent resource pools. Resource pools and virtual machines that are at the same level are called siblings. The cluster itself represents the root resource pool. If you do not create child resource pools, only the root resource pools exist.

In the following example, RP-QA is the parent resource pool for RP-QA-UI. RP-Marketing and RP-QA are siblings. The three virtual machines immediately below RP-Marketing are also siblings.

Figure 25-2. Parents, Children, and Siblings in Resource Pool Hierarchy



For each resource pool, you specify reservation, limit, shares, and whether the reservation should be expandable. The resource pool resources are then available to child resource pools and virtual machines.

Create a Resource Pool

You can create a child resource pool of any ESXi host, resource pool, or DRS cluster.

NOTE If a host has been added to a cluster, you cannot create child resource pools of that host. If the cluster is enabled for DRS, you can create child resource pools of the cluster.

When you create a child resource pool, you are prompted for resource pool attribute information. The system uses admission control to make sure you cannot allocate resources that are not available.

Prerequisites

The vSphere Client is connected to the vCenter Server system. If you connect the vSphere Client directly to a host, you cannot create a resource pool.

Procedure

1 In the vSphere Client inventory, select a parent object for the resource pool (a host, another resource pool, or a DRS cluster).

2 Select **File > New > Resource Pool**.

3 Type a name to identify the resource pool.

4 Specify how to allocate CPU and memory resources.

The CPU resources for your resource pool are the guaranteed physical resources the host reserves for a resource pool. Normally, you accept the default and let the host handle resource allocation.

Option	Description
Shares	Specify shares for this resource pool with respect to the parent's total resources. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. ■ Select **Low**, **Normal**, or **High** to specify share values respectively in a 1:2:4 ratio. ■ Select **Custom** to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Specify a guaranteed CPU or memory allocation for this resource pool. Defaults to 0. A nonzero reservation is subtracted from the unreserved resources of the parent (host or resource pool). The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool.
Expandable Reservation	When the check box is selected (default), expandable reservations are considered during admission control. If you power on a virtual machine in this resource pool, and the combined reservations of the virtual machines are larger than the reservation of the resource pool, the resource pool can use resources from its parent or ancestors.
Limit	Specify the upper limit for this resource pool's CPU or memory allocation. You can usually accept the default (**Unlimited**). To specify a limit, deselect the **Unlimited** check box.

5 Click **OK**.

After you create a resource pool, you can add virtual machines to it. A virtual machine's shares are relative to other virtual machines (or resource pools) with the same parent resource pool.

Example: Creating Resource Pools

Assume that you have a host that provides 6GHz of CPU and 3GB of memory that must be shared between your marketing and QA departments. You also want to share the resources unevenly, giving one department (QA) a higher priority. This can be accomplished by creating a resource pool for each department and using the **Shares** attribute to prioritize the allocation of resources.

The example shows how to create a resource pool with the ESXi host as the parent resource.

1 In the Create Resource Pool dialog box, type a name for the QA department's resource pool (for example, RP-QA).

2 Specify **Shares** of **High** for the CPU and memory resources of RP-QA.

3 Create a second resource pool, RP-Marketing.

Leave Shares at **Normal** for CPU and memory.

4 Click **OK**.

If there is resource contention, RP-QA receives 4GHz and 2GB of memory, and RP-Marketing 2GHz and 1GB. Otherwise, they can receive more than this allotment. Those resources are then available to the virtual machines in the respective resource pools.

Edit a Resource Pool

After you create the resource pool, you can edit its CPU and memory resource settings.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the resource pool in the inventory and select **Edit Settings**.

2 In the Edit Settings dialog box, you can change all attributes of the selected resource pool as described in "Create a Resource Pool," on page 353.

3 Click **OK** to save your changes.

Add a Virtual Machine to a Resource Pool

When you create a virtual machine, the New Virtual Machine wizard allows you to specify a resource pool location as part of the creation process. You can also add an existing virtual machine to a resource pool.

When you move a virtual machine to a new resource pool:

- The virtual machine's reservation and limit do not change.
- If the virtual machine's shares are high, medium, or low, %Shares adjusts to reflect the total number of shares in use in the new resource pool.
- If the virtual machine has custom shares assigned, the share value is maintained.

  NOTE Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares when you move it into a resource pool so that the virtual machine's shares are consistent with the relative values in the new resource pool. A warning appears if a virtual machine would receive a very large (or very small) percentage of total shares.

- The information displayed in the Resource Allocation tab about the resource pool's reserved and unreserved CPU and memory resources changes to reflect the reservations associated with the virtual machine (if any).

  NOTE If a virtual machine has been powered off or suspended, it can be moved but overall available resources (such as reserved and unreserved CPU and memory) for the resource pool are not affected.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the virtual machine in the inventory.

   The virtual machine can be associated with a standalone host, a cluster, or a different resource pool.

2 Drag the virtual machine (or machines) to the resource pool.

If a virtual machine is powered on, and the destination resource pool does not have enough CPU or memory to guarantee the virtual machine's reservation, the move fails because admission control does not allow it. An error dialog box displays available and requested resources, so you can consider whether an adjustment might resolve the issue.

Remove a Virtual Machine from a Resource Pool

You can remove a virtual machine from a resource pool either by moving the virtual machine to another resource pool or deleting it.

When you remove a virtual machine from a resource pool, the total number of shares associated with the resource pool decreases, so that each remaining share represents more resources. For example, assume you have a pool that is entitled to 6GHz, containing three virtual machines with shares set to **Normal**. Assuming the virtual machines are CPU-bound, each gets an equal allocation of 2GHz. If one of the virtual machines is moved to a different resource pool, the two remaining virtual machines each receive an equal allocation of 3GHz.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 Choose one of the following methods to remove the virtual machine from a resource pool.

- Drag the virtual machine to another resource pool.

  You do not need to power off the virtual machine before you move it.

- Right-click the virtual machine and select **Remove from Inventory** or **Delete from Disk**.

  You must power off the virtual machine before you can completely remove it.

Remove a Resource Pool

You can remove a resource pool from the inventory.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the resource pool and select **Remove**.

  A confirmation dialog box appears.

2 Click **Yes** to remove the resource pool.

Using DRS Clusters to Manage Resources

After you create a DRS cluster, you can customize it and use it to manage resources.

To customize your DRS cluster and the resources it contains you can configure affinity rules and you can add and remove hosts and virtual machines. When a cluster's settings and resources have been defined, you should ensure that it is and remains a valid cluster. You can also use a valid DRS cluster to manage power resources and interoperate with vSphere HA.

Creating a DRS Cluster

A cluster is a collection of ESXi hosts and associated virtual machines with shared resources and a shared management interface. Before you can obtain the benefits of cluster-level resource management you must create a cluster and enable DRS.

Depending on whether or not Enhanced vMotion Compatibility (EVC) is enabled, DRS behaves differently when you use vSphere Fault Tolerance (vSphere FT) virtual machines in your cluster.

Table 25-1. DRS Behavior with vSphere FT Virtual Machines and EVC

EVC	DRS (Load Balancing)	DRS (Initial Placement)
Enabled	Enabled (Primary and Secondary VMs)	Enabled (Primary and Secondary VMs)
Disabled	Disabled (Primary and Secondary VMs)	Disabled (Primary VMs) Fully Automated (Secondary VMs)

Create a DRS Cluster

Create a DRS cluster using the New Cluster wizard in the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

You can create a cluster without a special license, but you must have a license to enable a cluster for vSphere DRS (or vSphere HA).

Procedure

1 Right-click a datacenter or folder in the vSphere Client and select **New Cluster**.

2 Name the cluster in the **Name** text box.

This name appears in the vSphere Client inventory panel.

3 Enable the DRS feature by clicking the **vSphere DRS** box.

You can also enable the vSphere HA feature by clicking **vSphere HA**.

4 Click **Next**.

5 Select a default automation level for DRS.

Automation Level	Action
Manual	■ Initial placement: Recommended host(s) is displayed. ■ Migration: Recommendation is displayed.
Partially Automated	■ Initial placement: Automatic. ■ Migration: Recommendation is displayed.
Fully Automated	■ Initial placement: Automatic. ■ Migration: Recommendation is executed automatically.

6 Set the migration threshold for DRS.

7 Click **Next**.

8 Specify the default power management setting for the cluster.

If you enable power management, select a vSphere DPM threshold setting.

9 Click **Next**.

10 If appropriate, enable Enhanced vMotion Compatibility (EVC) and select the mode it should operate in.

11 Click **Next**.

12 Select a location for the swapfiles of your virtual machines.

You can either store a swapfile in the same directory as the virtual machine itself, or a datastore specified by the host (host-local swap)

13 Click **Next**.

14 Review the summary page that lists the options you selected.

15 Click **Finish** to complete cluster creation, or click **Back** to go back and make modifications to the cluster setup.

A new cluster does not include any hosts or virtual machines.

To add hosts and virtual machines to the cluster see "Adding Hosts to a Cluster," on page 359 and "Removing Virtual Machines from a Cluster," on page 361.

Set a Custom Automation Level for a Virtual Machine

After you create a DRS cluster, you can customize the automation level for individual virtual machines to override the cluster's default automation level.

For example, you can select **Manual** for specific virtual machines in a cluster with full automation, or **Partially Automated** for specific virtual machines in a manual cluster.

If a virtual machine is set to **Disabled**, vCenter Server does not migrate that virtual machine or provide migration recommendations for it. This is known as pinning the virtual machine to its registered host.

Note If you have not enabled Enhanced vMotion Compatibility (EVC) for the cluster, fault tolerant virtual machines are set to DRS disabled. They appear on this screen, but you cannot assign an automation mode to them.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane under vSphere DRS, select **Virtual Machine Options**.

3 Select the **Enable individual virtual machine automation levels** check box.

4 (Optional) To temporarily disable any individual virtual machine overrides, deselect the **Enable individual virtual machine automation levels** check box.

   Virtual machine settings are restored when the check box is selected again.

5 (Optional) To temporarily suspend all vMotion activity in a cluster, put the cluster in manual mode and deselect the **Enable individual virtual machine automation levels** check box.

6 Select one or more virtual machines.

7 Click the **Automation Level** column and select an automation level from the drop-down menu.

Option	Description
Manual	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Partially Automated	Initial placement is performed automatically. Migration recommendations are displayed, but do not run.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

8 Click **OK**.

Note Other VMware products or features, such as vSphere vApp and vSphere Fault Tolerance, might override the automation levels of virtual machines in a DRS cluster. Refer to the product-specific documentation for details.

Disable DRS

You can turn off DRS for a cluster.

When DRS is disabled, the cluster's resource pool hierarchy and affinity rules are not reestablished when DRS is turned back on. So if you disable DRS, the resource pools are removed from the cluster. To avoid losing the resource pools, instead of disabling DRS, you should suspend it by changing the DRS automation level to manual (and disabling any virtual machine overrides). This prevents automatic DRS actions, but preserves the resource pool hierarchy.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the cluster in the vSphere Client inventory.

2 Right click and select **Edit Settings**.

3 In the left panel, select **General**, and deselect the **Turn On vSphere DRS** check box.

4 Click **OK** to turn off DRS.

Adding Hosts to a Cluster

The procedure for adding hosts to a cluster is different for hosts managed by the same vCenter Server (managed hosts) than for hosts not managed by that server.

After a host has been added, the virtual machines deployed to the host become part of the cluster and DRS can recommend migration of some virtual machines to other hosts in the cluster.

Add a Managed Host to a Cluster

When you add a standalone host already being managed by vCenter Server to a DRS cluster, the host's resources become associated with the cluster.

You can decide whether you want to associate existing virtual machines and resource pools with the cluster's root resource pool or graft the resource pool hierarchy.

NOTE If a host has no child resource pools or virtual machines, the host's resources are added to the cluster but no resource pool hierarchy with a top-level resource pool is created.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the host from either the inventory or list view.

2 Drag the host to the target cluster object.

3 Select what to do with the host's virtual machines and resource pools.

- **Put this host's virtual machines in the cluster's root resource pool**

  vCenter Server removes all existing resource pools of the host and the virtual machines in the host's hierarchy are all attached to the root. Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares after selecting this option, which destroys the resource pool hierarchy.

- **Create a resource pool for this host's virtual machines and resource pools**

vCenter Server creates a top-level resource pool that becomes a direct child of the cluster and adds all children of the host to that new resource pool. You can supply a name for that new top-level resource pool. The default is **Grafted from <host_name>**.

The host is added to the cluster.

Add an Unmanaged Host to a Cluster

You can add an unmanaged host to a cluster. Such a host is not currently managed by the same vCenter Server system as the cluster and it is not visible in the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the cluster to which to add the host and select **Add Host** from the right-click menu.

2 Enter the host name, user name, and password, and click **Next**.

3 View the summary information and click **Next**.

4 Select what to do with the host's virtual machines and resource pools.

- **Put this host's virtual machines in the cluster's root resource pool**

  vCenter Server removes all existing resource pools of the host and the virtual machines in the host's hierarchy are all attached to the root. Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares after selecting this option, which destroys the resource pool hierarchy.

- **Create a resource pool for this host's virtual machines and resource pools**

  vCenter Server creates a top-level resource pool that becomes a direct child of the cluster and adds all children of the host to that new resource pool. You can supply a name for that new top-level resource pool. The default is **Grafted from <host_name>**.

The host is added to the cluster.

Adding Virtual Machines to a Cluster

You can add a virtual machine to a cluster in three ways.

- When you add a host to a cluster, all virtual machines on that host are added to the cluster.
- When a virtual machine is created, the New Virtual Machine wizard prompts you for the location to place the virtual machine. You can select a standalone host or a cluster and you can select any resource pool inside the host or cluster.
- You can migrate a virtual machine from a standalone host to a cluster or from a cluster to another cluster using the Migrate Virtual Machine wizard. To start this wizard either drag the virtual machine object on top of the cluster object or right-click the virtual machine name and select **Migrate**.

  NOTE You can drag a virtual machine directly to a resource pool within a cluster. In this case, the Migrate Virtual Machine wizard is started but the resource pool selection page does not appear. Migrating directly to a host within a cluster is not allowed because the resource pool controls the resources.

Removing Virtual Machines from a Cluster

You can remove virtual machines from a cluster.

You can remove a virtual machine from a cluster in two ways.

- When you remove a host from a cluster, all of the powered-off virtual machines that you do not migrate to other hosts are removed as well. You can remove a host only if it is in maintenance mode or disconnected. If you remove a host from a DRS cluster, the cluster can become yellow because it is overcommitted.
- You can migrate a virtual machine from a cluster to a standalone host or from a cluster to another cluster using the Migrate Virtual Machine wizard. To start this wizard right-click the virtual machine name and select **Migrate**.

Removing a Host from a Cluster

When you remove a host from a DRS cluster, you affect resource pool hierarchies, virtual machines, and you might create invalid clusters. Consider the affected objects before you remove the host.

- Resource Pool Hierarchies – When you remove a host from a cluster, the host retains only the root resource pool, even if you used a DRS cluster and decided to graft the host resource pool when you added the host to the cluster. In that case, the hierarchy remains with the cluster. You can create a host-specific resource pool hierarchy.

  NOTE Ensure that you remove the host from the cluster by first placing it in maintenance mode. If you instead disconnect the host before removing it from the cluster, the host retains the resource pool that reflects the cluster hierarchy.

- Virtual Machines – A host must be in maintenance mode before you can remove it from the cluster and for a host to enter maintenance mode all powered-on virtual machines must be migrated off that host. When you request that a host enter maintenance mode, you are also asked whether you want to migrate all the powered-off virtual machines on that host to other hosts in the cluster.
- Invalid Clusters – When you remove a host from a cluster, the resources available for the cluster decrease. If the cluster has enough resources to satisfy the reservations of all virtual machines and resource pools in the cluster, the cluster adjusts resource allocation to reflect the reduced amount of resources. If the cluster does not have enough resources to satisfy the reservations of all resource pools, but there are enough resources to satisfy the reservations for all virtual machines, an alarm is issued and the cluster is marked yellow. DRS continues to run.

Place a Host in Maintenance Mode

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.

Virtual machines that are running on a host entering maintenance mode need to be migrated to another host (either manually or automatically by DRS) or shut down. The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered down or migrated to different hosts. You cannot power on virtual machines or migrate virtual machines to a host entering maintenance mode.

When no more running virtual machines are on the host, the host's icon changes to include **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.

NOTE DRS does not recommend (or perform, in fully automated mode) any virtual machine migrations off of a host entering maintenance or standby mode if the vSphere HA failover level would be violated after the host enters the requested mode.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory, right-click a host and select **Enter Maintenance Mode**.

- If the host is part of a partially automated or manual DRS cluster, a list of migration recommendations for virtual machines running on the host appears.
- If the host is part of an automated DRS cluster, virtual machines are migrated to different hosts when the host enters maintenance mode.

2 If applicable, click **Apply Recommendations**.

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

Remove a Host from a Cluster

You can remove hosts from a cluster.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the host in the inventory and select **Enter Maintenance Mode**.

2 When the host is in maintenance mode, drag it to a different inventory location, either the top-level datacenter or to a different cluster.

After you remove a host from a cluster, you can perform the following tasks.

- Remove the host from vCenter Server: Right-click the host and select **Remove**.
- Run the host as a standalone host under vCenter Server: Right-click the host and select **Exit Maintenance Mode**.
- Drag the host into another cluster.

When you move the host, its resources are removed from the cluster. If you grafted the host's resource pool hierarchy onto the cluster, that hierarchy remains with the cluster.

Using Standby Mode

When a host machine is placed in standby mode, it is powered off.

Normally, hosts are placed in standby mode by the vSphere DPM feature to optimize power usage. You can also place a host in standby mode manually. However, DRS might undo (or recommend undoing) your change the next time it runs. To force a host to remain off, place it in maintenance mode and power it off.

Managing Power Resources

The vSphere Distributed Power Management (DPM) feature allows a DRS cluster to reduce its power consumption by powering hosts on and off based on cluster resource utilization.

vSphere DPM monitors the cumulative demand of all virtual machines in the cluster for memory and CPU resources and compares this to the total available resource capacity of all hosts in the cluster. If sufficient excess capacity is found, vSphere DPM places one or more hosts in standby mode and powers them off after migrating their virtual machines to other hosts. Conversely, when capacity is deemed to be inadequate, DRS brings hosts out of standby mode (powers them on) and uses vMotion to migrate virtual machines to them. When making these calculations, vSphere DPM considers not only current demand, but it also honors any user-specified virtual machine resource reservations.

NOTE ESXi hosts cannot automatically be brought out of standby mode unless they are running in a cluster managed by vCenter Server.

vSphere DPM can use one of three power management protocols to bring a host out of standby mode: Intelligent Platform Management Interface (IPMI), Hewlett-Packard Integrated Lights-Out (iLO), or Wake-On-LAN (WOL). Each protocol requires its own hardware support and configuration. If a host does not support any of these protocols it cannot be put into standby mode by vSphere DPM. If a host supports multiple protocols, they are used in the following order: IPMI, iLO, WOL.

NOTE Do not disconnect a host in standby mode or move it out of the DRS cluster without first powering it on, otherwise vCenter Server is not able to power the host back on.

Configure IPMI or iLO Settings for vSphere DPM

IPMI is a hardware-level specification and Hewlett-Packard iLO is an embedded server management technology. Each of them describes and provides an interface for remotely monitoring and controlling computers.

You must perform the following procedure on each host.

Prerequisites

Both IPMI and iLO require a hardware Baseboard Management Controller (BMC) to provide a gateway for accessing hardware control functions, and allow the interface to be accessed from a remote system using serial or LAN connections. The BMC is powered-on even when the host itself is powered-off. If properly enabled, the BMC can respond to remote power-on commands.

If you plan to use IPMI or iLO as a wake protocol, you must configure the BMC. BMC configuration steps vary according to model. See your vendor’s documentation for more information. With IPMI, you must also ensure that the BMC LAN channel is configured to be always available and to allow operator-privileged commands. On some IPMI systems, when you enable "IPMI over LAN" you must configure this in the BIOS and specify a particular IPMI account.

vSphere DPM using only IPMI supports MD5- and plaintext-based authentication, but MD2-based authentication is not supported. vCenter Server uses MD5 if a host's BMC reports that it is supported and enabled for the Operator role. Otherwise, plaintext-based authentication is used if the BMC reports it is supported and enabled. If neither MD5 nor plaintext authentication is enabled, IPMI cannot be used with the host and vCenter Server attempts to use Wake-on-LAN.

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the host in the vSphere Client inventory.

2 Click the **Configuration** tab.

3 Click **Power Management**.

4 Click **Properties**.

5 Enter the following information.

- User name and password for a BMC account. (The user name must have the ability to remotely power the host on.)
- IP address of the NIC associated with the BMC, as distinct from the IP address of the host. The IP address should be static or a DHCP address with infinite lease.
- MAC address of the NIC associated with the BMC.

6 Click **OK**.

Test Wake-on-LAN for vSphere DPM

The use of Wake-on-LAN (WOL) for the vSphere DPM feature is fully supported, if you configure and successfully test it according to the VMware guidelines. You must perform these steps before enabling vSphere DPM for a cluster for the first time or on any host that is being added to a cluster that is using vSphere DPM.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Before testing WOL, ensure that your cluster meets the prerequisites.

- Your cluster must contain at least two ESX 3.5 (or ESX 3i version 3.5) or later hosts.
- Each host's vMotion networking link must be working correctly. The vMotion network should also be a single IP subnet, not multiple subnets separated by routers.
- The vMotion NIC on each host must support WOL. To check for WOL support, first determine the name of the physical network adapter corresponding to the VMkernel port by selecting the host in the inventory panel of the vSphere Client, selecting the **Configuration** tab, and clicking **Networking**. After you have this information, click on **Network Adapters** and find the entry corresponding to the network adapter. The **Wake On LAN Supported** column for the relevant adapter should show Yes.
- To display the WOL-compatibility status for each NIC on a host, select the host in the inventory panel of the vSphere Client, select the **Configuration** tab, and click **Network Adapters**. The NIC must show Yes in the **Wake On LAN Supported** column.
- The switch port that each WOL-supporting vMotion NIC is plugged into should be set to auto negotiate the link speed, and not set to a fixed speed (for example, 1000 Mb/s). Many NICs support WOL only if they can switch to 100 Mb/s or less when the host is powered off.

After you verify these prerequisites, test each ESXi host that is going to use WOL to support vSphere DPM. When you test these hosts, ensure that the vSphere DPM feature is disabled for the cluster.

Caution Ensure that any host being added to a vSphere DPM cluster that uses WOL as a wake protocol is tested and disabled from using power management if it fails the testing. If this is not done, vSphere DPM might power off hosts that it subsequently cannot power back up.

Procedure

1 Click the **Enter Standby Mode** command on the host's **Summary** tab in the vSphere Client.

This action powers down the host.

2 Try to bring the host out of standby mode by clicking the **Power On**command on the host's **Summary** tab.

3 Observe whether or not the host successfully powers back on.

4 For any host that fails to exit standby mode successfully, select the host in the cluster Settings dialog box's Host Options page and change its **Power Management** setting to Disabled.

After you do this, vSphere DPM does not consider that host a candidate for being powered off.

Using DRS Affinity Rules

You can control the placement of virtual machines on hosts within a cluster by using affinity rules.

You can create two types of rules.

- Used to specify affinity or anti-affinity between a group of virtual machines and a group of hosts. An affinity rule specifies that the members of a selected virtual machine DRS group can or must run on the members of a specific host DRS group. An anti-affinity rule specifies that the members of a selected virtual machine DRS group cannot run on the members of a specific host DRS group.

  See "VM-Host Affinity Rules," on page 367 for information about creating and using this type of rule.

- Used to specify affinity or anti-affinity between individual virtual machines. A rule specifying affinity causes DRS to try to keep the specified virtual machines together on the same host, for example, for performance reasons. With an anti-affinity rule, DRS tries to keep the specified virtual machines apart, for example, so that when a problem occurs with one host, you do not lose both virtual machines.

  See "VM-VM Affinity Rules," on page 366 for information about creating and using this type of rule.

When you add or edit an affinity rule, and the cluster's current state is in violation of the rule, the system continues to operate and tries to correct the violation. For manual and partially automated DRS clusters, migration recommendations based on rule fulfillment and load balancing are presented for approval. You are not required to fulfill the rules, but the corresponding recommendations remain until the rules are fulfilled.

To check whether any enabled affinity rules are being violated and cannot be corrected by DRS, select the cluster's **DRS** tab and click **Faults**. Any rule currently being violated has a corresponding fault on this page. Read the fault to determine why DRS is not able to satisfy the particular rule. Rules violations also produce a log event.

Note VM-VM and VM-Host affinity rules are different from an individual host's CPU affinity rules.

Create a Host DRS Group

A VM-Host affinity rule establishes an affinity (or anti-affinity) relationship between a virtual machine DRS group with a host DRS group. You must create both of these groups before you can create a rule that links them.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane of the cluster Settings dialog box under **vSphere DRS**, select **DRS Groups Manager**.

3 In the Host DRS Groups section, click **Add**.

4 In the DRS Group dialog box, type a name for the group.

5 In the left pane, select a host and click >> to add it to the group. Continue this process until all desired hosts have been added.

   You can also remove hosts from the group by selecting them in the right pane and clicking <<.

6 Click **OK**.

What to do next

Using this host DRS group, you can create a VM-Host affinity rule that establishes an affinity (or anti-affinity) relationship with an appropriate virtual machine DRS group.

"Create a Virtual Machine DRS Group," on page 366

"Create a VM-Host Affinity Rule," on page 367

Create a Virtual Machine DRS Group

Affinity rules establish an affinity (or anti-affinity) relationship between DRS groups. You must create DRS groups before you can create a rule that links them.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane of the cluster Settings dialog box under **vSphere DRS**, select **DRS Groups Manager**.

3 In the Virtual Machines DRS Groups section, click **Add**.

4 In the DRS Group dialog box, type a name for the group.

5 In the left pane, select a host and click >> to add it to the group. Continue this process until all desired hosts have been added.

   You can also remove hosts from the group by selecting them in the right pane and clicking <<.

6 Click **OK**.

What to do next

"Create a Host DRS Group," on page 365

"Create a VM-Host Affinity Rule," on page 367

"Create a VM-VM Affinity Rule," on page 366

VM-VM Affinity Rules

A VM-VM affinity rule specifies whether selected individual virtual machines should run on the same host or be kept on separate hosts. This type of rule is used to create affinity or anti-affinity between individual virtual machines that you select.

When an affinity rule is created, DRS tries to keep the specified virtual machines together on the same host. You might want to do this, for example, for performance reasons.

With an anti-affinity rule, DRS tries to keep the specified virtual machines apart. You could use such a rule if you want to guarantee that certain virtual machines are always on different physical hosts. In that case, if a problem occurs with one host, not all virtual machines would be placed at risk.

Create a VM-VM Affinity Rule

You can create VM-VM affinity rules in the Cluster Settings dialog box to specify whether selected individual virtual machines should run on the same host or be kept on separate hosts.

Note If you use the vSphere HA Specify Failover Hosts admission control policy and designate multiple failover hosts, VM-VM affinity rules are not supported.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane of the Cluster Settings dialog box under **vSphere DRS**, select **Rules**.

3 Click **Add**.

4 In the Rule dialog box, type a name for the rule.

5 From the **Type** menu, select either **Keep Virtual Machines Together** or **Separate Virtual Machines**.

6 Click **Add**.

7 Select at least two virtual machines to which the rule will apply and click **OK**.

8 Click **OK**.

VM-Host Affinity Rules

A VM-Host affinity rule specifies whether or not the members of a selected virtual machine DRS group can run on the members of a specific host DRS group.

Unlike a VM-VM affinity rule, which specifies affinity (or anti-affinity) between individual virtual machines, a VM-Host affinity rule specifies an affinity relationship between a group of virtual machines and a group of hosts. There are 'required' rules (designated by "must") and 'preferential' rules (designated by "should".)

A VM-Host affinity rule includes the following components.

- One virtual machine DRS group.
- One host DRS group.
- A designation of whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on").

Because VM-Host affinity rules are cluster-based, the virtual machines and hosts that are included in a rule must all reside in the same cluster. If a virtual machine is removed from the cluster, it loses its DRS group affiliation, even if it is later returned to the cluster.

Create a VM-Host Affinity Rule

You can create VM-Host affinity rules in the Cluster Settings dialog box to specify whether or not the members of a selected virtual machine DRS group can run on the members of a specific host DRS group.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Create the virtual machine and host DRS groups to which the VM-Host affinity rule applies.

Procedure

1 In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.

2 In the left pane of the Cluster Settings dialog box under vSphere DRS, select **Rules**.

3 Click **Add**.

4 In the Rule dialog box, type a name for the rule.

5 From the **Type** menu, select **Virtual Machines to Hosts**.

6 Select the virtual machine DRS group and the host DRS group to which the rule applies.

7 Select a specification for the rule.

- **Must run on hosts in group**. Virtual machines in VM Group 1 must run on hosts in Host Group A.
- **Should run on hosts in group**. Virtual machines in VM Group 1 should, but are not required, to run on hosts in Host Group A.
- **Must not run on hosts in group**. Virtual machines in VM Group 1 must never run on host in Host Group A.
- **Should not run on hosts in group**. Virtual machines in VM Group 1 should not, but might, run on hosts in Host Group A.

8 Click **OK**.

Creating a Datastore Cluster

A datastore cluster is a collection of datastores with shared resources and a shared management interface. Datastore clusters are to datastores what clusters are to hosts. When you create a datastore cluster, you can use vSphere Storage DRS to manage storage resources.

Note Datastore clusters are referred to as storage pods in the vSphere API.

When you add a datastore to a datastore cluster, the datastore's resources become part of the datastore cluster's resources. As with clusters of hosts, you use datastore clusters to aggregate storage resources, which enables you to support resource allocation policies at the datastore cluster level. The following resource management capabilities are also available per datastore cluster.

Space utilization load balancing	You can set a threshold for space use. When space use on a datastore exceeds the threshold, Storage DRS generates recommendations or performs Storage vMotion migrations to balance space use across the datastore cluster.
I/O latency load balancing	You can set an I/O latency threshold for bottleneck avoidance. When I/O latency on a datastore exceeds the threshold, Storage DRS generates recommendations or performs Storage vMotion migrations to help alleviate high I/O load.
Anti-affinity rules	You can create anti-affinity rules for virtual machine disks. For example, the virtual disks of a certain virtual machine must be kept on different datastores. By default, all virtual disks for a virtual machine are placed on the same datastore.

Create a Datastore Cluster

You can manage datastore cluster resources using Storage DRS.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the Datastores and Datastore Clusters view of the vSphere Client inventory, right-click the Datacenter object and select **New Datastore Cluster**.

2 Follow the prompts to complete the Create Datastore Cluster wizard.

Enable and Disable Storage DRS

Storage DRS allows you to manage the aggregated resources of a datastore cluster. When Storage DRS is enabled, it provides recommendations for virtual machine disk placement and migration to balance space and I/O resources across the datastores in the datastore cluster.

When you enable Storage DRS, you enable the following functions.

- Space load balancing among datastores within a datastore cluster.
- I/O load balancing among datastores within a datastore cluster.
- Initial placement for virtual disks based on space and I/O workload.

The Enable Storage DRS check box in the Datastore Cluster Settings dialog box enables or disables all of these components at once. If necessary, you can disable I/O-related functions of Storage DRS independently of space balancing functions.

When you disable Storage DRS on a datastore cluster, Storage DRS settings are preserved. When you enable Storage DRS, the settings for the datastore cluster are restored to the point where Storage DRS was disabled.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.
2. Click **General**.
3. Select **Turn on Storage DRS** and click **OK**.
4. (Optional) To disable only I/O-related functions of Storage DRS, leaving space-related controls enabled, perform the following steps.
   a. Select **SDRS Runtime Rules**.
   b. Deselect the **Enable I/O metric for Storage DRS** check box.
5. Click **OK**.

Set the Automation Level for Datastore Clusters

The automation level for a datastore cluster specifies whether or not placement and migration recommendations from Storage DRS are applied automatically.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.
2. Select **SDRS Automation**.
3. Select an automation level.

   Manual is the default automation level.

Option	Description
No Automation (Manual Mode)	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.

4 Click **OK**.

Set Storage DRS Runtime Rules

Set Storage DRS triggers and configure advanced options for the datastore cluster.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 (Optional) Select or deselect the **Enable I/O metric for SDRS recommendations** check box to enable or disable I/O metric inclusion.

When you disable this option, vCenter Server does not consider I/O metrics when making Storage DRS recommendations. When you disable this option, you disable the following elements of Storage DRS:

- I/O load balancing among datastores within a datastore cluster.
- Initial placement for virtual disks based on I/O workload. Initial placement is based on space only.

2 (Optional) Set Storage DRS thresholds.

You set the aggressiveness level of Storage DRS by specifying thresholds for used space and I/O latency.

- Use the Utilized Space slider to indicate the maximum percentage of consumed space allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when space use on the datastores is higher than the threshold.
- Use the I/O Latency slider to indicate the maximum I/O latency allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when latency is higher than the threshold.

NOTE The Storage DRS I/O Latency threshold for the datastore cluster should be lower than or equal to the Storage I/O Control congestion threshold.

3 (Optional) Configure advanced options.

- No recommendations until utilization difference between source and destination is: Use the slider to specify the space utilization difference threshold. Utilization is usage * 100/capacity.

  This threshold ensures that there is some minimum difference between the space utilization of the source and the destination. For example, if the space used on datastore A is 82% and datastore B is 79%, the difference is 3. If the threshold is 5, Storage DRS will not make migration recommendations from datastore A to datastore B.
- Evaluate I/O load every: Specify how often Storage DRS should assess space and I/O load balancing.
- I/O imbalance threshold: Use the slider to indicate the aggressiveness of I/O load balancing. Lowering this value makes I/O load balancing less aggressive. Storage DRS computes an I/O fairness metric between 0 and 1, which 1 being the fairest distribution. I/O load balancing runs only if the computed metric is less than 1 - (I/O imbalance threshold / 100).

4 Click **Next**.

Adding and Removing Datastores from a Datastore Cluster

You add and remove datastores to and from an existing datastore cluster by dragging them in the vSphere Client inventory.

You can add to a datastore cluster any datastore that is mounted on a host in the vSphere Client inventory, with the following exceptions:

- All hosts attached to the datastore must be ESXi 5.0 and later.
- The datastore cannot be in more than one datacenter in the same instance of the vSphere Client.

When you remove a datastore from a datastore cluster, the datastore remains in the vSphere Client inventory and is not unmounted from the host.

Using Datastore Clusters to Manage Storage Resources

After you create a datastore cluster, you can customize it and use it to manage storage I/O and space utilization resources.

Using Storage DRS Maintenance Mode

You place a datastore in maintenance mode when you need to take it out of use to service it. A datastore enters or leaves maintenance mode only as the result of a user request.

Maintenance mode is available to datastores within a Storage DRS-enabled datastore cluster. Standalone datastores cannot be placed in maintenance mode.

Virtual disks that are located on a datastore that is entering maintenance mode must be migrated to another datastore, either manually or using Storage DRS. When you attempt to put a datastore in maintenance mode, the **Placement Recommendations** tab displays a list of migration recommendations, datastores within the same datastore cluster where virtual disks can be migrated. On the **Faults** tab, vCenter Server displays a list of the disks that cannot be migrated and the reasons why. If Storage DRS affinity or anti-affinity rules prevent disks from being migrated, you can choose to enable the Ignore Affinity Rules for Maintenance option.

The datastore is in a state of Entering Maintenance Mode until all virtual disks have been migrated.

Place a Datastore in Maintenance Mode

If you need to take a datastore out of service, you can place the datastore in Storage DRS maintenance mode.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Storage DRS is enabled on the datastore cluster that contains the datastore that is entering maintenance mode.

No CD-ROM image files are stored on the datastore.

There are at least two datastores in the datastore cluster.

Procedure

1 In the vSphere Client inventory, right-click a datastore in a datastore cluster and select **Enter SDRS Maintenance Mode**.

   A list of recommendations appears for datastore maintenance mode migration.

2 (Optional) On the Placement Recommendations tab, deselect any recommendations you do not want to apply.

NOTE The datastore cannot enter maintenance mode without evacuating all disks. If you deselect recommendations, you must manually move the affected virtual machines.

3 If necessary, click **Apply Recommendations**.

vCenter Server uses Storage vMotion to migrate the virtual disks from the source datastore to the destination datastore and the datastore enters maintenance mode.

The datastore icon might not be immediately updated to reflect the datastore's current state. To update the icon immediately, click **Refresh**.

Ignore Storage DRS Affinity Rules for Maintenance Mode

Storage DRS affinity or anti-affinity rules might prevent a datastore from entering maintenance mode. You can ignore these rules when you put a datastore in maintenance mode.

When you enable the Ignore Affinity Rules for Maintenance option for a datastore cluster, vCenter Server ignores Storage DRS affinity and anti-affinity rules that prevent a datastore from entering maintenance mode.

Storage DRS rules are ignored only for evacuation recommendations. vCenter Server does not violate the rules when making space and load balancing recommendations or initial placement recommendations.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.

2 In the right pane of the Edit Datastore Cluster dialog box, select **SDRS Automation**.

3 Click **Advanced Options**.

4 Select **IgnoreAffinityRulesForMaintenance**.

5 In the Value column, type `1` to enable the option.

Type `0` to disable the option.

6 Click **OK**.

The Ignore Affinity Rules for Maintenance Mode option is applied to the datastore cluster.

Applying Storage DRS Recommendations

Storage DRS collects resource usage information for all datastores in a datastore cluster. Storage DRS uses the information to generate recommendations for virtual machine disk placement on datastores in a datastore cluster.

Storage DRS recommendations appear on the **Storage DRS** tab in the vSphere Client datastore view. Recommendations also appear when you attempt to put a datastore into Storage DRS maintenance mode. When you apply Storage DRS recommendations, vCenter Server uses Storage vMotion to migrate virtual machine disks to other datastores in the datastore cluster to balance the resources.

You can apply a subset of the recommendations by selecting the Override Suggested DRS Recommendations check box and selecting each recommendation to apply.

Table 25-2. Storage DRS Recommendations

Label	Description
Priority	Priority level (1-5) of the recommendation. (Hidden by default.)
Recommendation	Action being recommended by Storage DRS.
Reason	Why the action is needed.
Space Utilization % Before (source) and (destination)	Percentage of space used on the source and destination datastores before migration.
Space Utilization % After (source) and (destination)	Percentage of space used on the source and destination datastores after migration.
I/O Latency Before (source)	Value of I/O latency on the source datastore before migration.
I/O Latency Before (destination)	Value of I/O latency on the destination datastore before migration.

Refresh Storage DRS Recommendations

Storage DRS migration recommendations appear on the **Storage DRS** tab in the vSphere Client. You can refresh these recommendations by running Storage DRS.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

At least one datastore cluster must exist in the vSphere Client inventory.

Enable Storage DRS for the datastore cluster. The **Storage DRS** tab appears only if Storage DRS is enabled.

Procedure

1 In the vSphere Client datastore view, select the datastore cluster and click the **Storage DRS** tab.

2 Select the **Recommendations** view and click the **Run Storage DRS** link in the upper right corner.

The recommendations are updated. The Last Updated timestamp displays the time when Storage DRS recommendations were refreshed.

Change Storage DRS Automation Level for a Virtual Machine

You can override the datastore cluster-wide automation level for individual virtual machines. You can also override default virtual disk affinity rules.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.

2 Select **Virtual Machine Settings**.

3 Select a virtual machine.

4 In the Automation Level column, select an automation level for the virtual machine.

Option	Description
Default (Manual)	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

5 In the **Keep VMDKs together** column, deselect the check box to override default VMDK affinity.

See "Override VMDK Affinity Rules," on page 377.

6 Click **OK**.

Set Up Off-Hours Scheduling for Storage DRS

You can create a scheduled task to change Storage DRS settings for a datastore cluster so that migrations for fully automated datastore clusters are more likely to occur during off-peak hours.

You can create a scheduled task to change the automation level and aggressiveness level for a datastore cluster. For example, you might configure Storage DRS to run less aggressively during peak hours, when performance is a priority, to minimize the occurrence of storage migrations. During non-peak hours, Storage DRS can run in a more aggressive mode and be invoked more frequently.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Enable Storage DRS.

Procedure

1 In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.

2 In the Edit Datastore Cluster dialog box, click **SDRS Scheduling**.

3 Click **Add**.

4 Type the time and select the days for the task to run.

5 Click **Next**.

6 Specify the start settings for the task.

   a Type a description for the start settings.

   For example, `Change SDRS Configuration`.

   b Select an automation level.

   c To disable I/O metrics for Storage DRS recommendations, select the check box.

   When you disable I/O metrics for Storage DRS recommendations, I/O metrics are not considered as part of Storage DRS recommendations or automated migrations for the datastore cluster.

   d Set the Utilized Space threshold.

   Use the Utilized Space slider to indicate the maximum percentage of consumed space allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when space use on the datastores is higher than the threshold.

e Set the I/O latency threshold.

Use the I/O Latency slider to indicate the maximum I/O latency allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when latency is higher than the threshold.

NOTE The Storage DRS I/O Latency threshold for the datastore cluster should be lower than or equal to the Storage I/O Control congestion threshold.

f Set the I/O imbalance threshold.

Use the I/O Imbalance Threshold slider to indicate the aggressiveness of I/O load balancing. Storage DRS makes recommendations and performs migrations if the I/O load imbalance level exceeds the threshold.

7 Click **Next**.

8 Specify the end settings for the task.

- To restore the Storage DRS settings to the pre-task configuration, select the **Restore settings** check box.
- To specify settings other than the pre-task configuration, deselect the **Restore settings** check box.

9 Review the Ready to Complete page and click **Finish**.

The scheduled task runs at the specified time.

Storage DRS Anti-Affinity Rules

You can create Storage DRS anti-affinity rules to control which virtual disks should not be placed on the same datastore within a datastore cluster. By default, a virtual machine's virtual disks are kept together on the same datastore.

When you create an anti-affinity rule, it applies to the relevant virtual disks in the datastore cluster. Anti-affinity rules are enforced during initial placement and Storage DRS-recommendation migrations, but are not enforced when a migration is initiated by a user.

NOTE Anti-affinity rules do not apply to CD-ROM ISO image files that are stored on a datastore in a datastore cluster, nor do they apply to swapfiles that are stored in user-defined locations.

Inter-VM Anti-Affinity Rules	Specify which virtual machines should never be kept on the same datastore. See "Create Inter-VM Anti-Affinity Rules," on page 376.
Intra-VM Anti-Affinity Rules	Specify which virtual disks associated with a particular virtual machine must be kept on different datastores. See "Create Intra-VM Anti-Affinity Rules," on page 377.

If you move a virtual disk out of the datastore cluster, the affinity or anti-affinity rule no longer applies to that disk.

When you move virtual disk files into a datastore cluster that has existing affinity and anti-affinity rules, the following behavior applies:

- Datastore Cluster B has an intra-VM affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, any rule that applied to the virtual disk for a given virtual machine in Datastore Cluster A no longer applies. The virtual disk is now subject to the intra-VM affinity rule in Datastore Cluster B.

- Datastore Cluster B has an inter-VM anti-affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, any rule that applied to the virtual disk for a given virtual machine in Datastore Cluster A no longer applies. The virtual disk is now subject to the inter-VM anti-affinity rule in Datastore Cluster B.
- Datastore Cluster B has an intra-VM anti-affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, the intra-VM anti-affinity rule does not apply to the virtual disk for a given virtual machine because the rule is limited to only specified virtual disks in Datastore Cluster B.

NOTE Storage DRS rules might prevent a datastore from entering maintenance mode. You can choose to ignore Storage DRS rules for maintenance mode by enabling the Ignore Affinity Rules for Maintenance option.

Create Inter-VM Anti-Affinity Rules

You can create an anti-affinity rule to indicate that all virtual disks of certain virtual machines must be kept on different datastores. The rule applies to individual datastore clusters.

Virtual machines that participate in an inter-VM anti-affinity rule in a datastore cluster must be associated with an intra-VM affinity rule in the datastore cluster. The virtual machines must also comply with the intra-VM affinity rule.

If a virtual machine is subject to an inter-VM anti-affinity rule, the following behavior applies:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.
- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

No inter-VM anti-affinity rules are defined by default.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.
2. In the left pane of the Edit Datastore Cluster dialog box, select **Rules**.
3. Click **Add**.
4. Type a name for the rule.
5. From the Type menu, select **VM anti-affinity**.
6. Click **Add**.
7. Click **Select Virtual Machine**.
8. Select at least two virtual machines and click **OK**.
9. Click **OK** to save the rule.

Create Intra-VM Anti-Affinity Rules

You can create a VMDK anti-affinity rule for a virtual machine that indicates which of its virtual disks must be kept on different datastores.

VMDK anti-affinity rules apply to the virtual machine for which the rule is defined, not to all virtual machines. The rule is expressed as a list of virtual disks that are to be separated from one another.

If you attempt to set an intra-VM anti-affinity rule and an intra-VM affinity rule for a virtual machine, vCenter Server rejects the most recently defined rule.

If a virtual machine is subject to a VMDK anti-affinity rule, the following behavior applies:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.
- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

No intra-VM anti-affinity rules are defined by default.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.
2. In the left pane of the Edit Datastore Cluster dialog box, select **Rules**.
3. Click **Add**.
4. Type a name for the rule.
5. From the Type menu, select **VMDK anti-affinity**.
6. Click **Add**.
7. Click **Select Virtual Machine**.
8. Select a virtual machine and click **OK**.
9. Select at least two virtual disks to which the rule applies and click **OK**.
10. Click **OK** to save the rule.

Override VMDK Affinity Rules

VMDK affinity rules indicate that all virtual disks in a datastore cluster that are associated with a particular virtual machine are located on the same datastore in the datastore cluster. The rules apply to individual datastore clusters.

VMDK affinity rules are enabled by default for all virtual machines that are in a datastore cluster. You can override the default setting for the datastore cluster or for individual virtual machines.

Virtual machines that are subject to VMDK affinity rules have the following behavior:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.

- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

When you add a datastore to a datastore cluster that is enabled for Storage DRS, the VMDK affinity rule is disabled for any virtual machine that has virtual disks on that datastore if it also has virtual disks on other datastores.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client inventory, right-click a datastore cluster and select **Edit Settings**.

2 Click **Virtual Machine Settings**.

3 Deselect the **Keep VMDKs together** check box for the virtual machine.

4 Click **OK**.

Clear Storage DRS Statistics

To diagnose problems with Storage DRS, you can clear Storage DRS statistics before you manually run Storage DRS.

Important When you enable the option to clear Storage DRS statistics, statistics are cleared every time Storage DRS runs until you disable the option. Always disable the option after you diagnose the Storage DRS problem.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Enable Storage DRS for the datastore cluster.

Procedure

1 Enable the `ClearIoStatsOnSdrsRun` option.

   a In the vSphere Client, right-click the datastore cluster and select **Edit Settings**.

   b Select **SDRS Automation Level** and click **Advanced Options**.

   c In the Option text box, type `ClearIoStatsOnSdrsRun`.

   d In the corresponding Value text box, type `1`.

   e Click **OK**, then click **OK** again to dismiss the settings dialog box.

2 In the vSphere Client inventory, select a datastore cluster.

3 Click the **Storage DRS** tab and select **Run DRS** in the upper right corner of the page.

   The current Storage DRS statistics for all datastores and virtual disks in all datastore clusters in the vSphere Client inventory are cleared, but no new statistics are collected.

4 Change the `ClearIoStatsOnSdrsRun` flag value to `0` to disable it.

5 Run Storage DRS again.

   Storage DRS runs normally. Allow several hours for the new setting to take effect.

Using NUMA Systems with ESXi

ESXi supports memory access optimization for Intel and AMD Opteron processors in server architectures that support NUMA (non-uniform memory access).

After you understand how ESXi NUMA scheduling is performed and how the VMware NUMA algorithms work, you can specify NUMA controls to optimize the performance of your virtual machines.

Change the Number of Virtual CPUs

You can configure a virtual machine that runs on an ESXi host to have up to 64 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

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.

2 Click the **Hardware** tab and select **CPUs**.

3 Select a value from the **Number of virtual sockets** drop-down menu.

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

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

5 Click **OK**.

Associate Virtual Machines with Specific Processors

You might be able to improve the performance of the applications on a virtual machine by pinning its virtual CPUs to fixed processors. This allows you to prevent the virtual CPUs from migrating across NUMA nodes.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.

2 Select the **Resources** tab, and select **Advanced CPU**.

3 In the Scheduling Affinity panel, set the CPU affinity to the preferred processors.

   Note You must manually select the boxes for all processors in the NUMA node. CPU affinity is specified on a per-processor, not on a per-node, basis.

Associate Memory Allocations with Specific NUMA Nodes Using Memory Affinity

You can specify that all future memory allocations on a virtual machine use pages associated with specific NUMA nodes (also known as manual memory affinity).

NOTE Specify nodes to be used for future memory allocations only if you have also specified CPU affinity. If you make manual changes only to the memory affinity settings, automatic NUMA rebalancing does not work properly.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.

2 Select the **Resources** tab, and select **Memory**.

3 In the NUMA Memory Affinity panel, set memory affinity.

Example: Binding a Virtual Machine to a Single NUMA Node

The following example illustrates manually binding the last four physical CPUs to a single NUMA node for a two-way virtual machine on an eight-way server.

The CPUs (for example, 4, 5, 6, and 7) are the physical CPU numbers.

1 In the vSphere Client inventory panel, select the virtual machine and select **Edit Settings**.

2 Select **Options** and click **Advanced**.

3 Click the **Configuration Parameters** button.

4 In the vSphere Client, turn on CPU affinity for processors 4, 5, 6, and 7.

Then, you want this virtual machine to run only on node 1.

1 In the vSphere Client inventory panel, select the virtual machine and select **Edit Settings**.

2 Select **Options** and click **Advanced**.

3 Click the **Configuration Parameters** button.

4 In the vSphere Client, set memory affinity for the NUMA node to 1.

Completing these two tasks ensures that the virtual machine runs only on NUMA node 1 and, when possible, allocates memory from the same node.

Associate Virtual Machines with Specified NUMA Nodes

When you associate a NUMA node with a virtual machine to specify NUMA node affinity, you constrain the set of NUMA nodes on which NUMA can schedule a virtual machine's virtual CPU and memory.

NOTE When you constrain NUMA node affinities, you might interfere with the ability of the ESXi NUMA scheduler to rebalance virtual machines across NUMA nodes for fairness. Specify NUMA node affinity only after you consider the rebalancing issues.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.

2 Click the **Options** tab.

3 Select **Advanced > General**.

4 Click **Configuration Parameters**.

5 Click **Add Row** to add a new option.

6 In the Name column, enter `numa.nodeAffinity`.

7 In the Value column, enter the NUMA nodes where the virtual machine can be scheduled.

   Use a comma-separated list for multiple nodes. For example, enter `0,1` to constrain the virtual machine resource scheduling to NUMA nodes 0 and 1.

8 Click **OK**.

9 Click **OK** to close the Virtual Machine Properties dialog box.

Advanced Attributes

You can set advanced attributes for hosts or individual virtual machines to help you customize resource management.

In most cases, adjusting the basic resource allocation settings (reservation, limit, shares) or accepting default settings results in appropriate resource allocation. However, you can use advanced attributes to customize resource management for a host or a specific virtual machine.

Set Advanced Host Attributes

You can set advanced attributes for a host.

Caution Changing advanced options is considered unsupported unless VMware technical support or a KB article instruct you to do so. In all other cases, changing these options is considered unsupported. In most cases, the default settings produce the optimum result.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the host in the inventory.

2 Click the **Configuration** tab.

3 Under **Software**, click **Advanced Settings**.

4 In the Advanced Settings dialog box, select the appropriate item (for example, **CPU** or **Mem**).

5 Locate the attribute in the right panel and edit the value.

6 Click **OK**.

Set Advanced Virtual Machine Attributes

You can set advanced attributes for a virtual machine.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, right-click the virtual machine in the inventory and select **Edit Settings**.

2 Click **Options** and click **Advanced > General**.

3 Click **Configuration Parameters**.

4 In the dialog box that appears, click **Add Row** to enter a new parameter and its value.

5 Click **OK**.

Creating and Using vSphere HA Clusters 26

vSphere HA clusters enable a collection of ESXi hosts to work together so that, as a group, they provide higher levels of availability for virtual machines than each ESXi host can provide individually. When you plan the creation and usage of a new vSphere HA cluster, the options you select affect the way that cluster responds to failures of hosts or virtual machines.

Before you create a vSphere HA cluster, you should know how vSphere HA identifies host failures and isolation and how it responds to these situations. You also should know how admission control works so that you can choose the policy that fits your failover needs. After you establish a cluster, you can customize its behavior with advanced options and optimize its performance by following recommended best practices.

NOTE You might get an error message when you try to use vSphere HA. For information about error messages related to vSphere HA, see the VMware knowledge base article at http://kb.vmware.com/kb/1033634.

This chapter includes the following topics:

- "vSphere HA Checklist," on page 383
- "Creating and Configuring a vSphere HA Cluster," on page 384
- "Customize an Individual Virtual Machine in the vSphere Client," on page 389

vSphere HA Checklist

The vSphere HA checklist contains requirements that you must be aware of before creating and using a vSphere HA cluster.

Review this list before you set up a vSphere HA cluster. For more information, follow the appropriate cross reference.

- All hosts must be licensed for vSphere HA.
- A cluster must contain at least two hosts.
- All hosts must be configured with static IP addresses. If you are using DHCP, you must ensure that the address for each host persists across reboots.
- All hosts must have at least one management network in common. The best practice is to have at least two management networks in common. You should use the VMkernel network with the **Management traffic** checkbox enabled. The networks must be accessible to each other and vCenter Server and the hosts must be accessible to each other on the management networks. See the *vSphere Availability* publication for best practices.

- To ensure that any virtual machine can run on any host in the cluster, all hosts must have access to the same virtual machine networks and datastores. Similarly, virtual machines must be located on shared, not local, storage otherwise they cannot be failed over in the case of a host failure.

  NOTE vSphere HA uses datastore heartbeating to distinguish between partitioned, isolated, and failed hosts. So if some datastores are more reliable in your environment, configure vSphere HA to give preference to them.

- For VM Monitoring to work, VMware tools must be installed. See the *vSphere Availability* publication for more information on VM and application monitoring.
- vSphere HA supports both IPv4 and IPv6. See the *vSphere Availability* publication for more information on vSphere HA interoperability.
- For VM Component Protection to work, hosts must have the All Paths Down (APD) Timeout feature enabled.
- To use VM Component Protection, clusters must contain ESXi 6.0 hosts or later.
- Only vSphere HA clusters that contain ESXi 6.0 or later hosts can be used to enable VMCP. Clusters that contain hosts from an earlier release cannot enable VMCP, and such hosts cannot be added to a VMCP-enabled cluster.
- If your cluster uses Virtual Volume (vVol) datastores, when vSphere HA is enabled a configuration vVol is created on each vVol datastore by vCenter Server. In these containers, vSphere HA stores the files it uses to protect virtual machines. vSphere HA does not function correctly if you delete these containers. Only one container is created per vVol datastore.

Creating and Configuring a vSphere HA Cluster

vSphere HA operates in the context of a cluster of ESXi (or legacy ESX) hosts. You must create a cluster, populate it with hosts, and configure vSphere HA settings before failover protection can be established.

When you create a vSphere HA cluster, you must configure a number of settings that determine how the feature works. Before you do this, identify your cluster's nodes. These nodes are the ESXi hosts that will provide the resources to support virtual machines and that vSphere HA will use for failover protection. You should then determine how those nodes are to be connected to one another and to the shared storage where your virtual machine data resides. After that networking architecture is in place, you can add the hosts to the cluster and finish configuring vSphere HA.

You can enable and configure vSphere HA before you add host nodes to the cluster. However, until the hosts are added, your cluster is not fully operational and some of the cluster settings are unavailable. For example, the Specify a Failover Host admission control policy is unavailable until there is a host that can be designated as the failover host.

NOTE The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

Create a vSphere HA Cluster in the vSphere Client

To enable your cluster for vSphere HA, first create an empty cluster. After you have planned the resources and networking architecture of your cluster, you can use the vSphere Client to add hosts to the cluster and specify the cluster's vSphere HA settings.

Open a vSphere Client connection to a to vCenter Server using an account with cluster administrator permissions.

Prerequisites

Verify that all virtual machines and their configuration files reside on shared storage. Verify that the hosts are configured to access that shared storage so that you can power on the virtual machines using different hosts in the cluster,

Verify that hosts are configured to have access to the virtual machine network.

NOTE Use redundant management network connections for vSphere HA. For information about network redundancy best practices, see the *vSphere Availability* publication. You should also configure hosts with at least two datastores to provide redundancy for vSphere HA datastore heartbeating.

Procedure

1 Select the Hosts & Clusters view.

2 Right-click the Datacenter in the Inventory tree and click **New Cluster**.

3 Complete the New Cluster wizard.

   Do not enable vSphere HA (or DRS) at this time.

4 Click **Finish** to close the wizard and create the cluster.

   You have created an empty cluster.

5 Based on your plan for the resources and networking architecture of the cluster, use the vSphere Client to add hosts to the cluster.

6 Right-click the cluster and click **Edit Settings**.

   The cluster's Settings dialog box is where you can modify the vSphere HA (and other) settings for the cluster.

7 On the Cluster Features page, select **Turn On vSphere HA**.

8 Configure the vSphere HA settings as appropriate for your cluster.

   - Host Monitoring Status
   - Admission Control
   - Virtual Machine Options
   - VM Monitoring
   - Datastore Heartbeating

9 Click **OK** to close the cluster's Settings dialog box.

You have a configured vSphere HA cluster, populated with hosts, available. For information about configuring the cluster settings, see "Configuring vSphere HA Cluster Settings in the vSphere Client," on page 386.

NOTE A vSphere HA-enabled cluster is a prerequisite for Fault Tolerance.

Configuring vSphere HA Cluster Settings in the vSphere Client

When you create a vSphere HA cluster or configure an existing cluster, you must configure settings that determine how the feature works.

In the vSphere Client, you can configure the following vSphere HA settings:

Host Monitoring Enable host monitoring to allow hosts in the cluster to exchange network heartbeats and to allow vSphere HA to take action when it detects failures.

> **NOTE** Host Monitoring is required for the vSphere Fault Tolerance recovery process to work properly.

Admission Control Enable or disable admission control for the vSphere HA cluster and choose a policy for how it is enforced.

Virtual Machine Options Set the VM restart priority and host isolation response.

VM Monitoring Enable VM Monitoring or VM and Application Monitoring.

Datastore Heartbeating Specify preferences for the datastores that vSphere HA uses for datastore heartbeating.

Configure Host Monitoring and Admission Control

After you create a cluster, Host Monitoring enables the vSphere HA master host to respond to host or virtual machine failures and management network isolation. Admission control allows you to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources to allow failover for all running virtual machines on the specified number of hosts.

The Host Monitoring and Admission Control page appears only if you enabled vSphere HA.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1. In the vSphere Client, display the cluster in the inventory.
2. Right-click the cluster and select **Edit Settings**.
3. In the left pane of the Cluster Settings dialog box, select **vSphere HA**.
4. (Optional) Select **Enable Host Monitoring**.
5. Select an Admission Control option.
   - Enable: Disallow VM power on operations that violate availability constraints.

     Enabling admission control enforces availability constraints and preserves failover capacity. Any operation on a virtual machine that decreases the unreserved resources in the cluster and violates availability constraints is not permitted.
   - Disable: Allow VM power on operations that violate availability constraints.

Disabling admission control allows a virtual machine to be powered on even if it causes insufficient failover capacity. When this happens, no warnings are presented, and the cluster does not turn red. If a cluster has insufficient failover capacity, vSphere HA can still perform failovers and it uses the VM Restart Priority setting to determine which virtual machines to power on first.

NOTE Select this option to power on more virtual machines than the vSphere HA failover level can support. If you select this option, failover is no longer guaranteed.

6 Select an admission control policy to apply to the cluster.

Option	Description
Host failures the cluster tolerates	Select the maximum number of host failures that you can recover from or to guarantee failover for.
Percentage of cluster resources reserved as failover spare capacity	Specify a percentage of the cluster's CPU and Memory resources to reserve as spare capacity to support failovers.
Specify failover hosts	Click to select hosts to use for failover actions. Failovers can still occur to other hosts in the cluster if a default failover host does not have enough resources.

7 (Optional) Select **Advanced Options** to configure automation mode options.

Change these settings only when instructed to do so by VMware technical support or when you are following specific instructions in VMware documentation.

8 Click **OK**.

Specify Failover Hosts

When you select the Specify Failover Hosts admission control policy, you must also designate which hosts are to be used for this function.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Open the Specify Failover Hosts dialog box from the vSphere HA screen of the Cluster Settings dialog box of the vSphere Client.

2 In the Available Hosts pane, select an available host to designate as a failover host.

3 Click the >> button to move the host name to the Failover Hosts pane.

4 Repeat steps 1 and 2 for each host you want to designate as a failover host.

5 To remove a host from the failover hosts list, select the name of that host in the Failover Hosts pane.

6 Click the << button to move the host name to the Available Hosts pane.

You can use the hosts designated as failover hosts to support the vSphere HA admission control process.

Set Virtual Machine Options

If you have enabled vSphere HA for a cluster, you can set the restart priority and host isolation response for virtual machines in the cluster.

The Virtual Machine Options page appears only if you enabled vSphere HA.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the **VM restart priority** for virtual machines in the cluster.

   The restart priority determines the order in which virtual machines are restarted when the host fails. Higher priority virtual machines are started first. This priority applies only on a per-host basis. If multiple hosts fail, all virtual machines are migrated from the first host in order of priority, then all virtual machines from the second host in order of priority, and so on.

2 Select the **Host isolation response**.

   The host isolation response determines what happens when a host in a vSphere HA cluster loses its console network connection but continues running.

3 Click **Next**.

Your virtual machine restart priority and host isolation response settings now take effect.

Configure VM and Application Monitoring

The Virtual Machine Monitoring feature uses the heartbeat information that VMware Tools captures as a proxy for guest operating system availability. This allows vSphere HA automatically to reset or restart individual virtual machines that have lost their ability to heartbeat.

The VM Monitoring page appears only if you enabled vSphere HA.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 (Optional) Select **VM Monitoring Only** to restart individual virtual machines if their heartbeats are not received within a set time. You can select **VM and Application Monitoring** if you also want to enable application monitoring.

2 Set the virtual machine monitoring sensitivity by moving the slider between **Low** and **High**. Select **Custom** to provide custom settings.

3 Click **Next**.

Configure Datastore Heartbeating

vSphere HA uses datastore heartbeating to distinguish between hosts that have failed and hosts that reside on a network partition. Datastore heartbeating allows vSphere HA to monitor hosts when a management network partition occurs and to continue to respond to failures that occur.

Use the Configure Datastore Heartbeating dialog box to specify the datastores that you want to be used for this purpose.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, display the cluster in the inventory.

2 Right-click the cluster and select **Edit Settings**.

3 In the left pane of the Cluster Settings dialog box, select **Datastore Heartbeating**.

4 To instruct vSphere HA about how to select the datastores and how to treat your preferences, choose from the following options:

Table 26-1.

Datastore Heartbeating Options
Select only from my preferred datastores
Select any of the cluster datastores
Select any of the cluster datastores taking into account my preferences

5 In the **Datastores Available for Heartbeating** pane, select the datastores that you want to use for heartbeating.

The datastores listed are those shared by more than one host in the vSphere HA cluster. When a datastore is selected, the lower pane displays all the hosts in the vSphere HA cluster that can access it.

6 Click **OK**.

Customize an Individual Virtual Machine in the vSphere Client

Each virtual machine in a vSphere HA cluster is assigned the cluster default settings for VM Restart Priority, Host Isolation Response, and VM Monitoring. You can specify specific behavior for each virtual machine by changing these defaults. If the virtual machine leaves the cluster, these settings are lost.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the cluster and select **Edit Settings** from the right-click menu.

2 Select **Virtual Machine Options** under vSphere HA.

3 In the Virtual Machine Settings pane, select a virtual machine and customize its **VM Restart Priority** or **Host Isolation Response** setting.

4 Select **VM Monitoring** under vSphere HA.

5 In the Virtual Machine Settings pane, select a virtual machine and customize its **VM Monitoring** setting.

6 Click **OK**.

The virtual machine's behavior now differs from the cluster defaults for each setting you changed.

Providing Fault Tolerance for Virtual Machines 27

You can utilize vSphere Fault Tolerance for your virtual machines to ensure business continuity with higher levels of availability and data protection than is offered by vSphere HA.

Fault Tolerance is built on the ESXi host platform, and it provides continuous availability by having identical virtual machines run on separate hosts.

To obtain the optimal results from Fault Tolerance you should be familiar with how it works, how to enable it for your cluster and virtual machines, and the best practices for its usage.

This chapter includes the following topics:

- "Fault Tolerance Use Cases," on page 391
- "Fault Tolerance Checklist," on page 392
- "Preparing Your Cluster and Hosts for Fault Tolerance," on page 393
- "Using Fault Tolerance," on page 396
- "Viewing Information About Fault Tolerant Virtual Machines in the vSphere Client," on page 398
- "Best Practices for Fault Tolerance," on page 400

Fault Tolerance Use Cases

Several typical situations can benefit from the use of vSphere Fault Tolerance.

Fault Tolerance provides a higher level of business continuity than vSphere HA. When a Secondary VM is called upon to replace its Primary VM counterpart, the Secondary VM immediately takes over the Primary VM's role with the entire state of the virtual machine preserved. Applications are already running, and data stored in memory does not need to be re-entered or reloaded. This differs from a failover provided by vSphere HA, which restarts the virtual machines affected by a failure.

This higher level of continuity and the added protection of state information and data informs the scenarios when you might want to deploy Fault Tolerance.

- Applications that need to be available at all times, especially those that have long-lasting client connections that users want to maintain during hardware failure.
- Custom applications that have no other way of doing clustering.
- Cases where high availability might be provided through custom clustering solutions, which are too complicated to configure and maintain.

Another key use case for protecting a virtual machine with Fault Tolerance can be described as On-Demand Fault Tolerance. In this case, a virtual machine is adequately protected with vSphere HA during normal operation. During certain critical periods, you might want to enhance the protection of the virtual machine. For example, you might be executing a quarter-end report which, if interrupted, might delay the availability

of mission critical information. With vSphere Fault Tolerance, you can protect this virtual machine prior to running this report and then turn off or suspend Fault Tolerance after the report has been produced. You can use On-Demand Fault Tolerance to protect the virtual machine during a critical time period and return the resources to normal during non-critical operation.

Fault Tolerance Checklist

The following checklist contains cluster, host, and virtual machine requirements that you need to be aware of before using vSphere Fault Tolerance.

Review this list before setting up Fault Tolerance.

NOTE The failover of fault tolerant virtual machines is independent of vCenter Server, but you must use vCenter Server to set up your Fault Tolerance clusters.

Cluster Requirements for Fault Tolerance

You must meet the following cluster requirements before you use Fault Tolerance.

- Fault Tolerance logging and VMotion networking configured. See "Configure Networking for Host Machines in the vSphere Client," on page 393.
- vSphere HA cluster created and enabled. See "Creating and Configuring a vSphere HA Cluster," on page 384. vSphere HA must be enabled before you can power on fault tolerant virtual machines or add a host to a cluster that already supports fault tolerant virtual machines.

Host Requirements for Fault Tolerance

You must meet the following host requirements before you use Fault Tolerance.

- Hosts must use supported processors.
- Hosts must be licensed for Fault Tolerance.
- Hosts must be certified for Fault Tolerance. See http://www.vmware.com/resources/compatibility/search.php and select **Search by Fault Tolerant Compatible Sets** to determine if your hosts are certified.
- The configuration for each host must have Hardware Virtualization (HV) enabled in the BIOS.

NOTE VMware recommends that the hosts you use to support FT VMs have their BIOS power management settings turned to "Maximum performance" or "OS-managed performance".

To confirm the compatibility of the hosts in the cluster to support Fault Tolerance, you can also run profile compliance checks as described in "Create Cluster and Check Compliance in the vSphere Client," on page 395.

Virtual Machine Requirements for Fault Tolerance

You must meet the following virtual machine requirements before you use Fault Tolerance.

- No unsupported devices attached to the virtual machine. See the *vSphere Availability* publication for more information on Fault Tolerance Interoperability.
- Incompatible features must not be running with the fault tolerant virtual machines. See the *vSphere Availability* publication for more information on Fault Tolerance Interoperability.
- Virtual machine files must be stored on shared storage. Acceptable shared storage solutions include Fibre Channel, (hardware and software) iSCSI, NFS, and NAS.

Other Configuration Recommendations

You should also observe the following guidelines when configuring Fault Tolerance.

- If you are using NFS to access shared storage, use dedicated NAS hardware with at least a 1Gbit NIC to obtain the network performance required for Fault Tolerance to work properly.
- The memory reservation of a fault tolerant virtual machine is set to the VM's memory size when Fault Tolerance is turned on. Ensure that a resource pool containing fault tolerant VMs has memory resources above the memory size of the virtual machines. Without this excess in the resource pool, there might not be any memory available to use as overhead memory.
- Use a maximum of 16 virtual disks per fault tolerant virtual machine.
- To ensure redundancy and maximum Fault Tolerance protection, you should have a minimum of three hosts in the cluster. In a failover situation, this provides a host that can accommodate the new Secondary VM that is created.

Preparing Your Cluster and Hosts for Fault Tolerance

To enable vSphere Fault Tolerance for your cluster, you must meet the feature's prerequisites and you must perform certain configuration steps on your hosts. After those steps are accomplished and your cluster has been created, you can also check that your configuration complies with the requirements for enabling Fault Tolerance.

The tasks you should complete before attempting to enable Fault Tolerance for your cluster include the following:

- Ensure that your cluster, hosts, and virtual machines meet the requirements outlined in the Fault Tolerance checklist.
- Configure networking for each host.
- Create the vSphere HA cluster, add hosts, and check compliance.

After your cluster and hosts are prepared for Fault Tolerance, you are ready to turn on Fault Tolerance for your virtual machines. See "Turn On Fault Tolerance for Virtual Machines in the vSphere Client," on page 396.

Configure Networking for Host Machines in the vSphere Client

On each host that you want to add to a vSphere HA cluster, you must configure two different networking switches so that the host can also support vSphere Fault Tolerance.

To enable Fault Tolerance for a host, you must complete this procedure twice, once for each port group option to ensure that sufficient bandwidth is available for Fault Tolerance logging. Select one option, finish this procedure, and repeat the procedure a second time, selecting the other port group option.

Prerequisites

Multiple gigabit Network Interface Cards (NICs) are required. For each host supporting Fault Tolerance, you need a minimum of two physical gigabit NICs. For example, you need one dedicated to Fault Tolerance logging and one dedicated to vMotion. Use three or more NICs to ensure availability.

Note The vMotion and FT logging NICs must be on different subnets and IPv6 is not supported on the FT logging NIC.

Procedure

1 Log in to the vSphere Client and select a host in the inventory pane.

2 Click the **Configuration** tab.

3 Select **Networking** under **Hardware**, and click the **Add Networking** link.

   The Add Network wizard appears.

4 Select **VMkernel** under **Connection Types** and click **Next**.

5 Select **Create a virtual switch** and click **Next**.

6 Provide a label for the switch.

7 Select either **Use this port group for vMotion** or **Use this port group for Fault Tolerance logging** and click **Next**.

8 Provide an IP address and subnet mask and click **Next**.

9 Click **Finish**.

After you create both a vMotion and Fault Tolerance logging virtual switch, you can create other virtual switches, as needed. You should then add the host to the cluster and complete any steps needed to turn on Fault Tolerance.

What to do next

To confirm that you successfully enabled both vMotion and Fault Tolerance on the host, view its **Summary** tab in the vSphere Client. In the General pane, the fields **vMotion Enabled** and **Host Configured for FT** should show yes.

NOTE If you configure networking to support FT but subsequently disable the Fault Tolerance logging port, pairs of fault tolerant virtual machines that are already powered on remain powered on. However, if a failover situation occurs, when the Primary VM is replaced by its Secondary VM a new Secondary VM is not started, causing the new Primary VM to run in a Not Protected state.

Fault Tolerance Host Networking Configuration Example

This example describes the host network configuration for Fault Tolerance in a typical deployment with four 1GB NICs. This is one possible deployment that ensures adequate service to each of the traffic types identified in the example and could be considered a best practice configuration.

Fault Tolerance provides full uptime during the course of a physical host failure due to power outage, system panic, or similar reasons. Network or storage path failures or any other physical server components that do not impact the host running state may not initiate a Fault Tolerance failover to the Secondary VM. Therefore, customers are strongly encouraged to use appropriate redundancy (for example, NIC teaming) to reduce that chance of losing virtual machine connectivity to infrastructure components like networks or storage arrays.

NIC Teaming policies are configured on the vSwitch (vSS) Port Groups (or Distributed Virtual Port Groups for vDS) and govern how the vSwitch will handle and distribute traffic over the physical NICs (vmnics) from virtual machines and vmkernel ports. A unique Port Group is typically used for each traffic type with each traffic type typically assigned to a different VLAN.

Figure 27-1 depicts the network configuration for a single ESXi host with four 1GB NICs supporting Fault Tolerance. Other hosts in the FT cluster would be configured similarly.

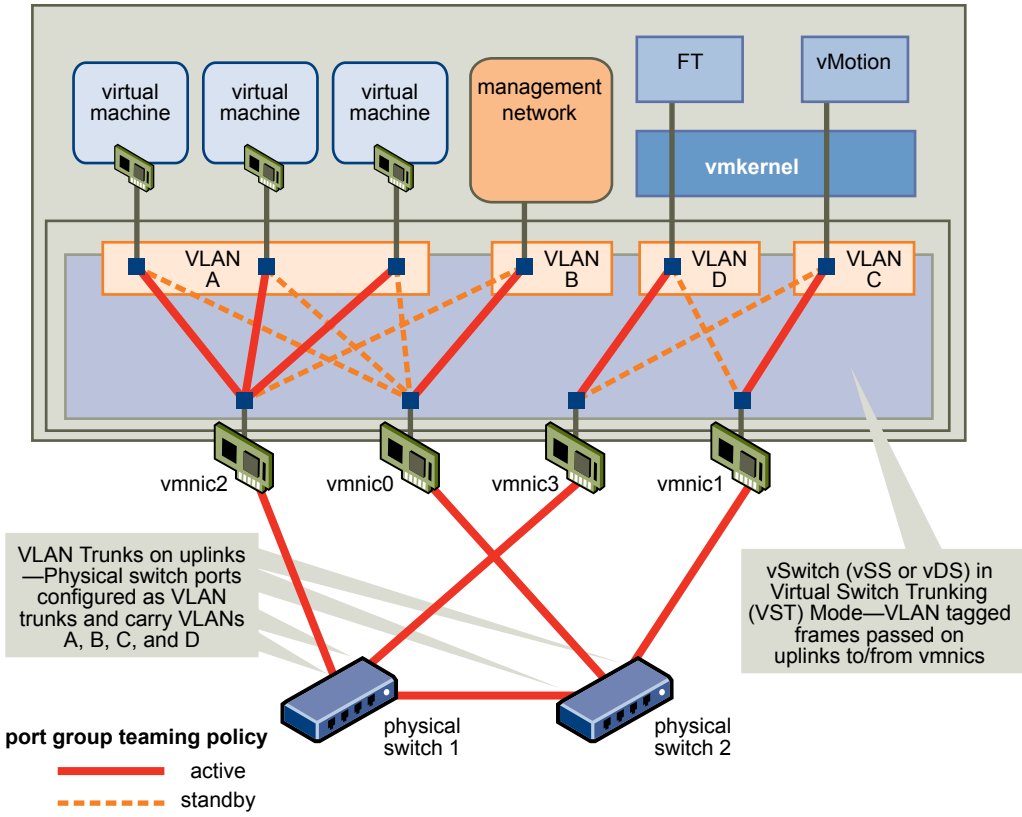
This example uses four port groups configured as follows:

- VLAN A: Virtual Machine Network Port Group-active on vmnic2 (to physical switch #1); standby on vmnic0 (to physical switch #2.)
- VLAN B: Management Network Port Group-active on vmnic0 (to physical switch #2); standby on vmnic2 (to physical switch #1.)

- VLAN C: vMotion Port Group-active on vmnic1 (to physical switch #2); standby on vmnic3 (to physical switch #1.)
- VLAN D: FT Logging Port Group-active on vmnic3 (to physical switch #1); standby on vmnic1 (to physical switch #2.)

vMotion and FT Logging can share the same VLAN (configure the same VLAN number in both port groups), but require their own unique IP addresses residing in different IP subnets. However, separate VLANs might be preferred if Quality of Service (QoS) restrictions are in effect on the physical network with VLAN based QoS. QoS is of particular use where competing traffic comes into play, for example, where multiple physical switch hops are used or when a failover occurs and multiple traffic types compete for network resources.

Figure 27-1. Fault Tolerance Networking Configuration Example



Create Cluster and Check Compliance in the vSphere Client

vSphere Fault Tolerance is used in the context of a vSphere HA cluster. After you have configured networking on each host, create the vSphere HA cluster and add the hosts to it. You can check to see if the cluster is configured correctly and complies with the requirements for the successful enablement of Fault Tolerance.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vCenter Server inventory, select the cluster and click the **Profile Compliance** tab.

2 Click **Check Compliance Now** to run the compliance tests.

To view the tests that are run, click **Description**.

The results of the compliance test appear at the bottom of the screen. A host is labeled as either Compliant or Noncompliant.

Using Fault Tolerance

After you have taken all of the required steps for enabling vSphere Fault Tolerance for your cluster, you can use the feature by turning it on for individual virtual machines.

Before Fault Tolerance can be turned on, validation checks are performed on a virtual machine.

After these checks are passed and you turn on vSphere Fault Tolerance for a virtual machine, new options are added to the Fault Tolerance section of its context menu. These include turning off or disabling Fault Tolerance, migrating the Secondary VM, testing failover, and testing restart of the Secondary VM.

Turn On Fault Tolerance for Virtual Machines in the vSphere Client

You can turn on vSphere Fault Tolerance through the vSphere Client.

When Fault Tolerance is turned on, vCenter Server unsets the virtual machine's memory limit and sets the memory reservation to the memory size of the virtual machine. While Fault Tolerance remains turned on, you cannot change the memory reservation, size, limit, or shares. When Fault Tolerance is turned off, any parameters that were changed are not reverted to their original values.

Prerequisites

Open a vSphere Client connection to a to vCenter Server using an account with cluster administrator permissions.

Procedure

1 Select the Hosts & Clusters view.

2 Right-click a single virtual machine and select **Fault Tolerance > Turn On Fault Tolerance**.

   If you select more than one virtual machine, the **Fault Tolerance** menu is disabled. You must turn Fault Tolerance on for one virtual machine at a time.

The specified virtual machine is designated as a Primary VM and a Secondary VM is established on another host. The Primary VM is now fault tolerant.

Setting Options for Fault Tolerant Virtual Machines in the vSphere Client

After you turn on vSphere Fault Tolerance for a virtual machine, new options are added to the Fault Tolerance section of its context menu.

In the vSphere Client, there are options for turning off or disabling Fault Tolerance, migrating the secondary virtual machine, testing failover, and testing restart of the secondary virtual machine.

Turn Off Fault Tolerance in the vSphere Client

Turning off vSphere Fault Tolerance deletes the secondary virtual machine, its configuration, and all history.

Use this option if you do not plan to reenable the feature. Otherwise, use the **Disable Fault Tolerance** option.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

If the Secondary VM resides on a host that is in maintenance mode, disconnected, or not responding, you cannot use the **Turn Off Fault Tolerance** option. In this case, you should disable and enable Fault Tolerance instead.

Procedure

1 In the vSphere Client, select the **Hosts & Clusters** view.

2 Right-click the fault tolerant virtual machine and select **Fault Tolerance > Turn Off Fault Tolerance**.

Fault Tolerance is turned off for the selected virtual machine. Any history and the secondary virtual machine for the selected virtual machine are deleted.

Disable Fault Tolerance in the vSphere Client

Disabling vSphere Fault Tolerance for a virtual machine suspends its Fault Tolerance protection, but preserves the Secondary VM, its configuration, and all history. Use this option if you might need to re-enable Fault Tolerance protection in the future.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the **Hosts & Clusters** view.

2 Right-click the fault tolerant virtual machine and select **Fault Tolerance > Disable Fault Tolerance**.

Fault Tolerance is disabled for the selected virtual machine. Any history and the Secondary VM for the selected virtual machine are preserved and will be used if the feature is re-enabled.

What to do next

After you have disabled Fault Tolerance, the menu option becomes **Enable Fault Tolerance**. Select this to re-enable the feature.

Migrate Secondary VM in the vSphere Client

After vSphere Fault Tolerance has been turned on for a Primary VM, you can change the host its associated Secondary VM resides on by migrating it.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the **Hosts & Clusters** view.

2 Right-click the fault tolerant virtual machine and select **Fault Tolerance > Migrate Secondary**.

   The Migrate Virtual Machine wizard opens with a Migration Type of **Change Host** selected.

3 Click **Next**.

4 Select the destination host that you want to migrate the Secondary VM to and click **Next**.

5 Select a migration priority and click **Next**.

6 Review your selections on the Summary page and click **Finish**.

The Secondary VM associated with the selected fault tolerant virtual machine is migrated to the specified host. Note that the Primary VM can always be migrated using the **Migrate** command in its context menu.

Test Fault Tolerance Failover in the vSphere Client

You can induce a failover situation for a selected Primary VM to test your Fault Tolerance protection.

This option is unavailable (grayed out) if the virtual machine is powered off.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the **Hosts & Clusters** view.

2 Right-click the fault tolerant virtual machine and select **Fault Tolerance > Test Failover**.

This task induces failure of the Primary VM to ensure that the Secondary VM replaces it. A new Secondary VM is also started placing the Primary VM back in a Protected state.

Test Restart Secondary VM in the vSphere Client

You can induce the failure of a Secondary VM to test the Fault Tolerance protection provided for a selected Primary VM.

This option is unavailable (grayed out) if the virtual machine is powered off.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the vSphere Client, select the **Hosts & Clusters** view.

2 Right-click the fault tolerant virtual machine and select **Fault Tolerance > Test Restart Secondary**.

This task results in the termination of the Secondary VM that provided Fault Tolerance protection for the selected Primary VM. A new Secondary VM is then started, placing the Primary VM back in a Protected state.

Viewing Information About Fault Tolerant Virtual Machines in the vSphere Client

You can view fault tolerant virtual machines in the vCenter Server inventory using the vSphere Client.

NOTE You cannot disable Fault Tolerance from the Secondary VM.

A vSphere Fault Tolerance section (pane) appears in the **Summary** tab for the Primary VM and includes information about the virtual machine.

Fault Tolerance Status Indicates the Fault Tolerance status of the virtual machine.

- Protected. The Primary and Secondary VMs are powered on and running as expected.

- Not Protected. The Secondary VM is not running. Possible reasons are listed in the table.

Table 27-1. Reasons for Primary VM Not Protected Status

Reason for Not Protected Status	Description
Starting	Fault Tolerance is in the process of starting the Secondary VM. This message is only visible for a short period of time.
Need Secondary VM	The Primary VM is running without a Secondary VM, so the Primary VM is currently not protected. This occurs when no compatible host in the cluster is available for the Secondary VM. Correct this by bringing a compatible host online. If a compatible host is online in the cluster, you might need to investigate further. Under certain circumstances, disabling Fault Tolerance and then re-enabling it corrects this problem.
Disabled	Fault Tolerance is currently disabled (no Secondary VM is running). This happens when Fault Tolerance is disabled by the user or when vCenter Server disables Fault Tolerance after being unable to power on the Secondary VM.
VM not Running	Fault Tolerance is enabled but the virtual machine is powered off. Power on the virtual machine to reach Protected state.

Secondary location Displays the ESXi host on which the Secondary VM is hosted.

Total Secondary CPU The CPU usage of the Secondary VM, displayed in MHz.

Total Secondary Memory The memory usage of the Secondary VM, displayed in MB.

vLockstep Interval The time interval (displayed in seconds) needed for the Secondary VM to match the current execution state of the Primary VM. Typically, this interval is less than one-half of one second. No state is lost during a failover, regardless of the vLockstep Interval value.

Log Bandwidth The amount of network capacity being used for sending vSphere Fault Tolerance log information from the host running the Primary VM to the host running the Secondary VM.

For each host configured to support Fault Tolerance, you can view information about its fault tolerant virtual machines by accessing the host's **Summary** tab in the vSphere Client. The **Fault Tolerance** section of this screen displays the total number of Primary and Secondary VMs residing on the host and the number of those virtual machines that are powered on. If the host is ESX/ESXi 4.1 or greater, this section also displays the Fault Tolerance version the host is running. Otherwise, it lists the host build number. For two hosts to be compatible they must have matching FT version numbers or matching host build numbers.

Best Practices for Fault Tolerance

To ensure optimal Fault Tolerance results, you should follow certain best practices.

The following recommendations for host and networking configuration can help improve the stability and performance of your cluster.

Host Configuration

Hosts running the Primary and Secondary VMs should operate at approximately the same processor frequencies, otherwise the Secondary VM might be restarted more frequently. Platform power management features that do not adjust based on workload (for example, power capping and enforced low frequency modes to save power) can cause processor frequencies to vary greatly. If Secondary VMs are being restarted on a regular basis, disable all power management modes on the hosts running fault tolerant virtual machines or ensure that all hosts are running in the same power management modes.

Host Networking Configuration

The following guidelines allow you to configure your host's networking to support Fault Tolerance with different combinations of traffic types (for example, NFS) and numbers of physical NICs.

- Distribute each NIC team over two physical switches ensuring L2 domain continuity for each VLAN between the two physical switches.
- Use deterministic teaming policies to ensure particular traffic types have an affinity to a particular NIC (active/standby) or set of NICs (for example, originating virtual port-id).
- Where active/standby policies are used, pair traffic types to minimize impact in a failover situation where both traffic types will share a vmnic.
- Where active/standby policies are used, configure all the active adapters for a particular traffic type (for example, FT Logging) to the same physical switch. This minimizes the number of network hops and lessens the possibility of oversubscribing the switch to switch links.

Note FT logging traffic between Primary and Secondary VMs is unencrypted and contains guest network and storage I/O data, as well as the memory contents of the guest operating system. This traffic can include sensitive data such as passwords in plaintext. To avoid such data being divulged, ensure that this network is secured, especially to avoid 'man-in-the-middle' attacks. For example, you could use a private network for FT logging traffic.

Homogeneous Clusters

vSphere Fault Tolerance can function in clusters with nonuniform hosts, but it works best in clusters with compatible nodes. When constructing your cluster, all hosts should have the following configuration:

- Common access to datastores used by the virtual machines.
- The same virtual machine network configuration.
- The same BIOS settings (power management and hyperthreading) for all hosts.

Run **Check Compliance** to identify incompatibilities and to correct them.

Performance

To increase the bandwidth available for the logging traffic between Primary and Secondary VMs use a 10Gbit NIC, and enable the use of jumbo frames.

Store ISOs on Shared Storage for Continuous Access

Store ISOs that are accessed by virtual machines with Fault Tolerance enabled on shared storage that is accessible to both instances of the fault tolerant virtual machine. If you use this configuration, the CD-ROM in the virtual machine continues operating normally, even when a failover occurs.

For virtual machines with Fault Tolerance enabled, you might use ISO images that are accessible only to the Primary VM. In such a case, the Primary VM can access the ISO, but if a failover occurs, the CD-ROM reports errors as if there is no media. This situation might be acceptable if the CD-ROM is being used for a temporary, noncritical operation such as a patch.

Avoid Network Partitions

A network partition occurs when a vSphere HA cluster has a management network failure that isolates some of the hosts from vCenter Server and from one another. See the *vSphere Availability* publication. When a partition occurs, Fault Tolerance protection might be degraded.

In a partitioned vSphere HA cluster using Fault Tolerance, the Primary VM (or its Secondary VM) could end up in a partition managed by a master host that is not responsible for the virtual machine. When a failover is needed, a Secondary VM is restarted only if the Primary VM was in a partition managed by the master host responsible for it.

To ensure that your management network is less likely to have a failure that leads to a network partition, follow the recommendations in the *vSphere Availability* publication.

Viewing Fault Tolerance Errors in the vSphere Client

When errors related to your implementation of Fault Tolerance are generated by vCenter Server, the Fault Details screen appears.

This screen lists faults related to Fault Tolerance and for each fault it provides the type of fault (red is an error, yellow is a warning), the name of the virtual machine or host involved, and a brief description.

You can also invoke this screen for a specific failed Fault Tolerance task. To do this, select the task in either the Recent Tasks pane or the **Tasks & Events** tab for the entity that experienced the fault and click the **View details** link that appears in the Details column.

Monitoring a Single Host with the vSphere Client 28

When you connect to a single host using the vSphere Client, you can monitor the host health status, and view events, system logs, and performance charts.

This chapter includes the following topics:

- "View Charts," on page 403
- "Working with Advanced and Custom Charts," on page 403
- "Monitoring Host Health Status," on page 406
- "Monitoring Events, Alarms, and Automated Actions," on page 408
- "Viewing Solutions," on page 422
- "Configure SNMP Settings for vCenter Server," on page 423
- "System Log Files," on page 424

View Charts

You can connect directly to ESX/ESXi hosts and view information about resource usage in line chart form.

Prerequisites

Connect to an ESX/ESXi host by using the vSphere Client.

Procedure

1 Select the host in the inventory.

2 Click the **Performance** tab.

3 Select a resource type from the **Switch to** drop-down menu.

4 (Optional) Click **Chart Options** to modify performance charts.

Working with Advanced and Custom Charts

Use advanced charts, or create your own custom charts, to see more performance data. Advanced charts can be useful when you are aware of a problem but need more statistical data to pinpoint the source of the trouble.

Advanced charts include the following features:

- More information. Hover over a data point in a chart and details about that specific data point are displayed.
- Customizable charts. Change chart settings. Save custom settings to create your own charts.

- Export to spreadsheet.
- Save to image file or spreadsheet.

Set Advanced Performance Charts as the Default

You can configure the vSphere Client to display the advanced performance charts by default when you open the **Performance** tab. The default is to display the overview performance charts.

Prerequisites

Ensure that you have connected to a vCenter Server system by using the vSphere Client.

Procedure

1 Select **Edit > Client Settings**.

2 In the **Tabs** section of the Client Settings dialog box, select **Default to Advanced Performance Charts**.

3 Click **OK**.

Change Performance Chart Settings

You can customize a performance chart by specifying the objects to monitor, the counters to include, the time range, and chart type. You can customize preconfigured chart views and create new chart views.

Prerequisites

Connect to a host through the vSphere Client.

Procedure

1 Select an inventory object and click the **Performance** tab.

2 Click **Chart Options**.

3 Select a metric group for the chart.

4 Select a time range for the metric group.

   If you choose **Custom**, do one of the following.

   - Select **Last** and set the number of hours, days, weeks, or months for the amount of time to monitor the object.
   - Select **From** and select the beginning and end dates.

   You can also customize the time range options by customizing the statistics collection interval setting.

5 Select the chart type.

   When selecting the stacked graph option, consider the following.

   - You can select only one item from the list of measurements.
   - Per-virtual-machine stacked graphs are available only for hosts.
   - Click a counter description name to display information about the counter's function and whether the selected metric can be stacked for per-virtual-machine graphs.

6 In Objects, select the inventory objects to display in the chart.

   You can also specify the objects using the **All** or **None** buttons.

7 In Counters, select the data counters to display in the chart.

   You can also specify counters using the **All** or **None** buttons.

   Click a counter name to display information about the counter in the Counter Description panel.

8 Click **Apply**.

   Changes to chart settings take effect immediately after they are applied.

9 Click **OK**.

Create a Custom Advanced Chart

You can create your own charts by saving customized chart settings. New charts are added to the **Switch to** menu and will appear there only when charts for the selected object are being displayed.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Customize chart settings as described in "Change Performance Chart Settings," on page 404.

2 Click **Save Chart Settings**.

3 Enter a name for your settings.

4 Click **OK**.

The chart settings are saved and an entry for your chart is added to the **Switch to** menu.

Delete a Custom Advanced Chart View

You can delete custom chart views from the vSphere Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select any object in the datacenter to enable the **Performance** tab.

2 Click the **Performance** tab and click **Advanced**.

3 Click **Chart Options**.

4 Click **Manage Chart Settings**.

5 Select a chart and click **Delete**.

   The chart is deleted, and it is removed from the **Switch to** menu.

6 Click **OK**.

Save Chart Data to a File

You can save data from the Advanced performance charts to a file in various graphics formats or in Microsoft Excel format.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 In the **Performance** tab, click **Advanced**.

2 Click **Save**.

3 In the Save Performance Chart dialog box, navigate to the location to save the file.

4 Enter a name for the file.

5 Select a file type.

6 Click **Save**.

The file is saved to the location and format you specified.

Export Performance Data to a Spreadsheet

You can export performance data from the Advanced charts to a Microsoft Office Excel file.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select the object in the inventory.

2 Select **File > Report > Performance**.

   If performance data is not available for the selected inventory object, the Export Performance option is not available.

3 Enter a filename and location.

4 Select the date and time range for the chart.

5 In **Chart Options**, select the chart type.

6 Select the metric groups to display in the chart.

   You can also specify the objects by selecting **All** or **None**.

7 (Optional) To customize the options, click **Advanced**, select the objects and counters to include in the chart, and click **OK**.

8 Specify the size of the chart in the exported file.

9 Click **OK** to export the data.

Monitoring Host Health Status

You can use the vSphere Web Client to monitor the state of host hardware components, such as CPU processors, memory, fans, and other components.

The host health monitoring tool allows you to monitor the health of a variety of host hardware components including:

- CPU processors
- Memory
- Fans
- Temperature
- Voltage

- Power
- Network
- Battery
- Storage
- Cable/Interconnect
- Software components
- Watchdog
- PCI devices
- Other

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware. SMASH is an industry standard specification providing protocols for managing a variety of systems in the data center. For more information, see http://www.dmtf.org/standards/smash.

You can monitor host health status either by connecting the vSphere Client directly to a host, or by connecting the vSphere Web Client to a vCenter Server system. You can also set alarms to trigger when the host health status changes.

NOTE The interpretation of hardware monitoring information is specific for each hardware vendor. Your hardware vendor can help you understand the results of the host hardware components monitoring.

Monitor Health Status When Directly Connected to a Host

When you connect the vSphere Client directly to a host, you can view the health status from the host's **Configuration** tab.

Prerequisites

Required privilege: **Host.Configuration.Advanced Configuration**

Procedure

1 Log in to the host using the vSphere Client, and display the inventory.

2 Click the **Configuration** tab, and click **Health Status**.

If a component is functioning normally, the status indicator is green. The status indicator changes to yellow or red if a system component violates a performance threshold or is not functioning properly. Generally, a yellow indicator signifies degraded performance. A red indicator signifies that a component stopped operating or exceeded the highest threshold. If the status is blank, then the health monitoring service cannot determine the status of the component.

The **Reading** column displays the current values for the sensors. For instance, the column displays rotations per minute (RPM) for fans and degrees Celsius for temperature.

Reset Hardware Sensors When Directly Connected to a Host

Some host hardware sensors display data that is cumulative over time. You can reset these sensors to clear the data in them and begin collecting new data.

Prerequisites

Launch the vSphere Client and log in to the ESXi host.

If you need to preserve sensor data for troubleshooting or other purposes, take a screenshot, export the data, or download a support bundle before resetting sensors.

Procedure

1 On the host **Configuration** tab, click **Health Status**.

2 Click **Sensor Refresh**.

Reset Health Status Sensors When Connected to vCenter Server

Some host hardware sensors display data that is cumulative over time. You can reset these sensors to clear the data in them and begin collecting new data.

If you need to preserve sensor data for troubleshooting or other purposes, take a screenshot, export the data, or download a support bundle before resetting sensors.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Ensure that the vCenter Hardware Status plug-in is enabled.

Procedure

1 Select a host in the object navigator or the iventory tree.

2 Click **Reset sensors**.

Monitoring Events, Alarms, and Automated Actions

vSphere includes a user-configurable events and alarms subsystem. This subsystem tracks events happening throughout vSphere and stores the data in log files and the vCenter Server database. This subsystem also enables you to specify the conditions under which alarms are triggered. Alarms can change state from mild warnings to more serious alerts as system conditions change, and can trigger automated alarm actions. This functionality is useful when you want to be informed, or take immediate action, when certain events or conditions occur for a specific inventory object, or group of objects.

Events

Events are records of user actions or system actions that occur on objects in vCenter Server or on a host. Actions that might be recordered as events include, but are not limited to, the following examples:

- A license key expires
- A virtual machine is powered on
- A user logs in to a virtual machine
- A host connection is lost

Event data includes details about the event such as who generated it, when it occured, and what type of event it is. There are three types of events:

- Information
- Warning
- Error

In the vSphere Client, event data is displayed in **Tasks and Events** tab for the selected inventory object. See "View Events," on page 410.

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. An alarm definition consists of the following elements:

- Name and description - Provides an identifying label and description.
- Alarm type - Defines the type of object that will be monitored.
- Triggers - Defines the event, condition, or state that will trigger the alarm and defines the notification severity.
- Tolerance thresholds (Reporting) - Provides additional restrictions on condition and state triggers thresholds that must be exceeded before the alarm is triggered.
- Actions - Defines operations that occur in response to triggered alarms. VMware provides sets of predefined actions that are specific to inventory object types.

Alarms have the following severity levels:

- Normal – green
- Warning – yellow
- Alert – red

Alarm definitions are associated with the object selected in the inventory. An alarm monitors the type of inventory objects specified in its definition.

For example, you might want to monitor the CPU usage of all virtual machines in a specific host cluster. You can select the cluster in the inventory, and add a virtual machine alarm to it. When enabled, that alarm will monitor all virtual machines running in the cluster and will trigger when any one of them meets the criteria defined in the alarm. If you want to monitor a specific virtual machine in the cluster, but not others, you would select that virtual machine in the inventory and add an alarm to it. One easy way to apply the same alarms to a group of objects is to place those objects in a folder and define the alarm on the folder.

Note You can enable, disable, and modify alarms only from the object in which the alarm is defined. For example, if you defined an alarm in a cluster to monitor virtual machines, you can only enable, disable, or modify that alarm through the cluster; you can not make changes to the alarm at the individual virtual machine level.

Alarm Actions

Alarm actions are operations that occur in response to the trigger. For example, you can have an email notification sent to one or more administrators when an alarm is triggered.

Note Default alarms are not preconfigured with actions. You must manually set what action occurs when the triggering event, condition, or state occurs.

View Events

You can either view all vSphere events or view events associated with a single object. The events list for a selected inventory object includes events associated with child objects.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Read-only**

Procedure

- To see a list of events associated with a selected inventory object and its child objects, select the **Tasks & Events** tab and click **Events**.
  - a Select an event to see event details.
  - b Use the filter controls above the list to filter the list.
  - c Click a column heading to sort the list.

View System Logs

System log entries include such information as who generated the event, when the event was created, and the type of event.

Prerequisites

Connect to an ESX/ESXi host by using the vSphere Client.

Required privilege:**Global. Diagnostics** privilege.

Procedure

1. To view system log entries, select **Home > Administration > System Logs**.
2. From the drop-down menu, select the log.
3. (Optional) Click **Show All** or **Show next # lines** to see additional log entries.
4. (Optional) Filter the log entries.
   - a Select **View > Filtering**.
   - b Type the filter criteria in the filter box.

Export Events Data

You can export all or part of the events data stored in the vCenter Server database.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required Privilege: **Read-only**

Procedure

1. Select **File > Export > Export Events**.
2. (Linked-mode only) In the **vCenter Server** list, select the server where the events occurred.
3. Specify Events, Time, and Limits attributes for the events you want to export.
4. Specify a file name and location.

5 Click **OK**.

vCenter Server creates the file in the specified location. The file contains the **Type**, **Time**, and **Description** of the events.

View Triggered Alarms and Alarm Definitions

Triggered alarms are visible in several locations throughout the vSphere Client and vSphere Web Client.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

- To view all triggered alarms, click **Alarms** in the status bar.
- To view alarms triggered on an selected inventory object, select the **Alarms** tab > **Triggered Alarms**.
- To view a list of alarms associated with a selected inventory object, select the **Alarms** tab > **Definitions**. The **Defined In** column indicates the object on which the alarm was set.

Set An Alarm

You can monitor inventory objects by setting alarms on them. Setting an alarm involves selecting the type of inventory object to monitor, defining when and for how long the alarm will trigger, and defining actions that will be performed as a result of the alarm being triggered. You define alarms in the Alarm Settings dialog box.

Prerequisites

Ensure that you have connected to a vCenter Server system by using the vSphere Client.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

- View and Edit Alarm Settings on page 412

  You create and modify alarms in the Alarm Settings dialog box. You can view alarm settings from any object, but you can modify settings only through the object on which the alarm is defined.

- Specify Alarm Name, Description, and Type on page 412

  General settings include alarm Name, Description, and Type. You can also enable and disable the alarm in the General settings tab. Specifying the alarm type includes selecting the type of inventory object and the type of activity (events, or conditions and states) that you want to monitor. The options in the Triggers tab change depending on the type of activity you choose to monitor.

- Specify How the Alarm is Triggered (Condition or State-based) on page 413

  You can specify the events, states, or conditions that triggers the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

- Specify How the Alarm is Triggered (Event-based) on page 414

  You can specify the events, states, or conditions that trigger the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

- Specify Alarm Tolerance and Frequency on page 414

  You can use reporting to apply a tolerance range for the alarm triggers. This can help you distinguish temporary problems from more serious, chronic ones. The Reporting settings allow you to specify the amount a condition or state must exceed the trigger value before the alarm triggers.

- Specify Which Actions to Perform When Triggered on page 415

  You can specify actions that the system performs when the alarm is triggered or changes status. You can enable and disable alarms and alarm actions independently of each other.

- Enable and Disable Alarm Actions on page 421

  You can disable alarm actions on any inventory object. Disabling alarm actions is not the same as disabling an alarm, nor is it the same as acknowledging an alarm. When alarm actions are disabled, the alarm can still be triggered but its associated actions will not be performed. You might want to disable alarm actions when, for example, you plan on putting a host into maintenance mode. When you disable alarm actions on a selected inventory object, all actions for all alarms are disabled on that object. You cannot disable a subset of alarm actions. Alarm actions will continue on the child objects.

View and Edit Alarm Settings

You create and modify alarms in the Alarm Settings dialog box. You can view alarm settings from any object, but you can modify settings only through the object on which the alarm is defined.

Prerequisites

Ensure that you have connected to a vCenter Server system by using the vSphere Client.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

◆ To view or change alarm settings, open the Alarm Settings dialog box:

Option	Description
Create New Alarm	Select an inventory object and select **File > New > Alarm**.
Add Alarm to Object	Right-click an inventory object and select **Alarm > Add Alarm**.
View Alarm Definitions	Select the **Alarms** tab, click the **Definitions** subtab of the inventory item with the alarm you want, and double-click an alarm in the list.

Specify Alarm Name, Description, and Type

General settings include alarm Name, Description, and Type. You can also enable and disable the alarm in the General settings tab. Specifying the alarm type includes selecting the type of inventory object and the type of activity (events, or conditions and states) that you want to monitor. The options in the Triggers tab change depending on the type of activity you choose to monitor.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 Right-click an inventory object and select **Alarms > Add Alarm**.

2 Enter a name and description.

3 Select the type of inventory object this alarm will monitor.

4 Select the type of activity this alarm will monitor.

   The options in the **Triggers** tab change depending on the type of activity you select.

5 Click **OK** to save your changes and exit the dialog box or select a different tab to make further changes to the alarm.

What to do next

NOTE You cannot save an alarm without triggers defined for it.

Specify How the Alarm is Triggered (Condition or State-based)

You can specify the events, states, or conditions that triggers the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Open the Triggers tab of the Alarm Settings dialog box. See "Specify Alarm Name, Description, and Type," on page 412.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 Select the trigger you want to change or click **Add** to add a new trigger.

2 Click in the **Trigger Type** column and select an option from the drop-down menu.

3 Click in the **Condition** column and select an option from the drop-down menu.

4 Click in the **Warning** column and select an option from the drop-down menu to set the threshold for triggering a warning.

5 (Optional) Click in the **Condition Length** column and select an option from the drop-down menu.

6 Click in the **Alert** column and select an option from the drop-down menu to set the threshold for triggering an alert.

7 (Optional) Click in the **Condition Length** column and select an option from the drop-down menu.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or optionally add more triggers, or configure any of the following settings:for this alarm:

- Repeat alarm thresholds
- Repeat alarm frequency
- Alarm actions
- Alarm action frequency

Specify How the Alarm is Triggered (Event-based)

You can specify the events, states, or conditions that trigger the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Open the Triggers tab of the Alarm Settings dialog box.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 Select the trigger you want to change or click **Add** to add a new trigger.

2 Click in the **Event** column and select an option from the drop-down menu.

3 Click in the **Status** column and select an option from the drop-down menu.

4 (Optional) Click **Advanced** in the **Conditions** column to configure additional conditions that must be met before the alarm triggers.

   a Click **Add** to add an argument.

   b Click in the **Argument** column and select an option from the drop-down menu.

   c Click in the **Operator** column and select an option from the drop-down menu.

   d Click in the **Value** column and enter a value into the text field.

   e Add more arguments, or click **OK** to exit the dialog box and return to the Alarm Settings dialog box.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or optionally add more triggers or configure alarm actions.

Specify Alarm Tolerance and Frequency

You can use reporting to apply a tolerance range for the alarm triggers. This can help you distinguish temporary problems from more serious, chronic ones. The Reporting settings allow you to specify the amount a condition or state must exceed the trigger value before the alarm triggers.

Reporting settings include Range and Frequency. Range is the threshold the monitored condition or state must exceed the specified trigger limit for the alarm to trigger. Frequency is the length of time between each re-triggering for as long as the condition or state exists. The **Reporting** tab is disabled for alarms with event-based triggers.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Open the Reporting tab of the Alarm Settings dialog box.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 (Optional) Specify how far over, or under, trigger limits the conditions must exceed before the alarm is triggered again.

2 (Optional) Select a **Frequency**.

The frequency sets the time period during which a triggered alarm is not reported again. When the time period has elapsed, the alarm will report again if the condition or state is still true.

What to do next

Optionally specify alarm actions, or click **OK** to save your changes and exit the dialog box.

Specify Which Actions to Perform When Triggered

You can specify actions that the system performs when the alarm is triggered or changes status. You can enable and disable alarms and alarm actions independently of each other.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Open the Actions tab of the Alarm Settings dialog box.

Ensure the vCenter Server is properly configured to use SNMP email or trap notifications as an alarm action.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

- Send Email as an Alarm Action on page 416

  You can use the SMTP agent included with vCenter Server to send email notifications when alarms are triggered.

- Send SNMP Traps as an Alarm Action on page 417

  The SNMP agent included with vCenter Server can be used to send traps when alarms are triggered on a vCenter Server. The default hardware health alarms send SNMP traps by default.

- Run a Script or a Command as an Alarm Action on page 418

  You can configure an alarm to run a script or a command when the alarm is triggered.

Procedure

1 Select the action that you want to change or click **Add** to add one.

2 Click in the **Action** column and select an option from the drop-down menu.

3 Click in the **Configuration** column and enter configuration information for those actions that require additional information:

Option	Action
Send a notification email	Enter email addresses, separated by a comma, and press **Enter**.
Migrate a VM	Complete the Migrate Virtual Machine wizard .
Run a command	Take one of the following actions and press **Enter**: ■ If the command is a `.exe` file, enter the full path name of the command and include any parameters. For example, to run the `cmd.exe` command in the `C:\tools` directory, with the `alarmName` and `targetName` parameters, type: **`c:\tools\cmd.exe alarmName targetName`** ■ If the command is a `.bat` file, enter the full path name of the command as an argument to the `c:\windows\system32\cmd.exe` command. Include any parameters. For example, to run the `cmd.bat` command in the `C:\tools` directory, with the `alarmName` and `targetName` parameters, type: **`c:\windows\system32\cmd.exe /c c:\tools\cmd.bat alarmName targetName`** For `.bat` files, the command and its parameters must be formatted into one string.

4 (Optional) For each alarm status change column, specify whether the alarm should be triggered when the alarm status changes.

Some actions do not support re-triggering on alarm status change.

5 For repeat actions, enter the time interval for the repetition in **Repeat After**.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

Send Email as an Alarm Action

You can use the SMTP agent included with vCenter Server to send email notifications when alarms are triggered.

Prerequisites

Ensure that the vCenter Server SMTP agent is properly configured to send email notifications.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 In the Actions tab of the Alarm Settings dialog box, click Add to add an action.

2 In the **Actions** column, select**Send a notification email** from the drop-down menu.

3 In the **Configuration** column, enter recipient addresses. Use commas to separate multiple addresses.

4 (Optional) Configure alarm transitions and frequency. See "Specify Which Actions to Perform When Triggered," on page 415.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

vCenter Server Email Agent Notifications

The following tables describe the information that is included in Alarm-based and Event-based email notifications. The first table described the information included in all email notifications; the second table describes additional information that is included in Event-based notifications.

Table 28-1. Basic SNMP Email Notification Details

Email Entry	Description
Target	Object for which the alarm was triggered.
Old Status	Previous alarm status. Applies only to state triggers.
New Status	Current alarm status. Applies only to state triggers.
Metric Value	Threshold value that triggered the alarm. Applies only to metric condition triggers.
Alarm Definition	Alarm definition in vCenter Server, including the alarm name and status.
Description	Localized string containing a summary of the alarm. For example: `Alarm New_Alarm on host1.vmware.com changed from Gray to Red.`

Table 28-2. Additional Notification Details for Alarms Triggered by Events

Detail	Description
Event Details	VMODL event type name.
Summary	Alarm summary, including the event type, alarm name, and target object.
Date	Time and date the alarm was triggered.
UserName	Person who initiated the action that caused the event to be created. Events caused by an internal system activity do not have a UserName value.
Host	Host on which the alarm was triggered.
Resource Pool	Resource pool on which the alarm was triggered.
Datacenter	Data center on which the alarm was triggered.
Arguments	Arguments passed with the alarm and their values.

Send SNMP Traps as an Alarm Action

The SNMP agent included with vCenter Server can be used to send traps when alarms are triggered on a vCenter Server. The default hardware health alarms send SNMP traps by default.

Prerequisites

Ensure that vCenter Server SNMP agents and ESXi SNMP agents are properly configured.

Ensure that SNMP trap receiver agents are properly configured.

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 In the Actions tab of the Alarm Settings dialog box, click **Add**.

2 In the **Actions** column, select **Send a notification trap** from the drop-down menu.

3 (Optional) Configure alarm transitions and frequency.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

SNMP Trap Notifications

The following table describes the information that is included in vCenter Server and ESXi trap notifications.

Table 28-3. SNMP Trap Notification Details

Trap Entry	Description
Type	The state vCenter Server is monitoring for the alarm. Options include Host Processor (or CPU) usage, Host Memory usage, Host State, Virtual Machine Processor (or CPU) usage, Virtual Machine Memory usage, Virtual Machine State, Virtual Machine Heartbeat.
Name	The name of the host or virtual machine that triggers the alarm.
Old Status	The alarm status before the alarm was triggered.
New Status	The alarm status when the alarm is triggered.
Object Value	The object value when the alarm is triggered.

Run a Script or a Command as an Alarm Action

You can configure an alarm to run a script or a command when the alarm is triggered.

Use the alarm environment variables to define complex scripts and attach them to multiple alarms or inventory objects. For example, you can write a script that enters the following trouble ticket information into an external system when an alarm is triggered:

- Alarm name
- Object on which the alarm was triggered
- Event that triggered the alarm
- Alarm trigger values

When you write the script, include the following environment variables in the script:

- VMWARE_ALARM_NAME
- VMWARE_ALARM_TARGET_NAME
- VMWARE_ALARM_EVENTDESCRIPTION
- VMWARE_ALARM_ALARMVALUE

You can attach the script to any alarm on any object without changing the script.

Prerequisites

Required Privilege: **Alarms.Create alarm** or **Alarms.Modify alarm**

Procedure

1 In the Actions tab of the Alarm Settings dialog box, click **Add** to add an action.

2 In the **Actions** column, select **Run a command** from the drop-down menu.

3 In the **Configuration** column, type script or command information:

For this type of command...	Enter this...
EXE executable files	Full pathname of the command. For example, to run the `cmd.exe` command in the `C:\tools` directory, type: **`c:\tools\cmd.exe`**.
BAT batch file	Full pathname of the command as an argument to the `c:\windows\system32\cmd.exe` command. For example, to run the `cmd.bat` command in the `C:\tools` directory, type: **`c:\windows\system32\cmd.exe /c c:\tools\cmd.bat`**. NOTE The command and its parameters must be formatted into one string.

If your script does not make use of the alarm environment variables, include any necessary parameters in the configuration field. For example:

```
c:\tools\cmd.exe AlarmName targetName
c:\windows\system32\cmd.exe /c c:\tools\cmd.bat alarmName targetName
```

4 (Optional) Configure alarm transitions and frequency. See "Specify Which Actions to Perform When Triggered," on page 415.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

Alarm Environment Variables for Scripts

To simplify script configuration for alarm actions, VMware provides environment variables for VMware alarms. Use the variables to define more complex scripts and attach them to multiple alarms or inventory objects so that the alarm action occurs when the alarm triggers.

Table 28-4. Alarm Environment Variables

Variable Name	Variable Description	Supported Alarm Type
VMWARE_ALARM_NAME	The name of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_ID	The MOID of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_TARGET_NAME	The name of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_TARGET_ID	The MOID of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_OLDSTATUS	The old status of the alarm.	Condition, State, Event
VMWARE_ALARM_NEWSTATUS	The new status of the alarm.	Condition, State, Event
VMWARE_ALARM_TRIGGERINGSUMMARY	A multiline summary of the alarm.	Condition, State, Event
VMWARE_ALARM_DECLARINGSUMMARY	A single-line declaration of the alarm expression.	Condition, State, Event
VMWARE_ALARM_ALARMVALUE	The value that triggered the alarm.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	A description of the alarm status change event.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	A description of the event that triggered the alarm.	Event

Table 28-4. Alarm Environment Variables (Continued)

Variable Name	Variable Description	Supported Alarm Type
VMWARE_ALARM_EVENT_USERNAME	The user name associated with the event.	Event
VMWARE_ALARM_EVENT_DATACENTER	The name of the data center in which the event occurred.	Event
VMWARE_ALARM_EVENT_COMPUTERESOURCE	The name of the cluster or resource pool in which the event occurred.	Event
VMWARE_ALARM_EVENT_HOST	The name of the host on which the event occurred.	Event
VMWARE_ALARM_EVENT_VM	The name of the virtual machine on which the event occurred.	Event
VMWARE_ALARM_EVENT_NETWORK	The name of the network on which the event occurred.	Event
VMWARE_ALARM_EVENT_DATASTORE	The name of the datastore on which the event occurred.	Event
VMWARE_ALARM_EVENT_DVS	The name of the vSphere Distributed Switch on which the event occurred.	Event

Alarm Command-Line Parameters

VMware provides command-line parameters that function as a substitute for the default alarm environment variables. You can use these parameters when running a script as an alarm action for a condition, state, or event alarm.

The command-line parameters enable you to pass alarm information without having to change an alarm script. For example, you can use these parameters when you have an external program for which you do not have the source. You can pass in the necessary data by using the substitution parameters, which take precedence over the environment variables. You pass the parameters through the **Configuration** dialog box in the alarm definition wizard or on a command line.

Table 28-5. Command-Line Parameters for Alarm Action Scripts

Variable	Description
`{eventDescription}`	The text of the alarmStatusChange event. The `{eventDescription}` variable is supported only for Condition and State alarms.
`{targetName}`	The name of the entity on which the alarm is triggered.
`{alarmName}`	The name of the alarm that is triggered.
`{triggeringSummary}`	A summary of the alarm trigger values.
`{declaringSummary}`	A summary of the alarm declaration values.
`{oldStatus}`	The alarm status before the alarm is triggered.
`{newStatus}`	The alarm status after the alarm is triggered.
`{target}`	The inventory object on which the alarm is set.

Enable and Disable Alarm Actions

You can disable alarm actions on any inventory object. Disabling alarm actions is not the same as disabling an alarm, nor is it the same as acknowledging an alarm. When alarm actions are disabled, the alarm can still be triggered but its associated actions will not be performed. You might want to disable alarm actions when, for example, you plan on putting a host into maintenance mode. When you disable alarm actions on a selected inventory object, all actions for all alarms are disabled on that object. You cannot disable a subset of alarm actions. Alarm actions will continue on the child objects.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Alarm.Disable Alarm Action**

Procedure

- To disable alarm actions, right-click on the inventory object and select **Alarm > Disable Alarm Actions**.
- To enable alarm actions, right click on the inventory object and select **Alarm > Enable Alarm Actions**.

Acknowledge Triggered Alarms

After an alarm is acknowledged, its alarm actions are discontinued. Alarms are neither cleared, nor reset when acknowledged.

Acknowledging an alarm lets other users know that you are taking ownership of the issue. For example, a host has an alarm set on it that monitors CPU usage and that sends an email to an administrator when the alarm is triggered. The host CPU usage spikes, triggering the alarm which sends an email to the host's administrator. The administrator acknowledges the triggered alarm to let other administrators know he is working on the problem, and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Alarm.Alarm Acknowledge**

Procedure

1. Navigate to the inventory panel.
2. If the status panel is not available, select **View > Status Bar** to view the status pane.
3. In the status bar, click **Alarms** to display the Triggered Alarms panel.
4. Right-click the alarm and select **Acknowledge Alarm**.

   To acknowledge multiple alarms at one time, Shift+click each alarm to select it, right-click the selection, and select **Acknowledge Alarm**.

Reset Triggered Event Alarms

An alarm triggered by an event might not reset to a normal state if vCenter Server does not retrieve the event that identifies the normal condition. In such cases, reset the alarm manually to return it to a normal state.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Required privilege: **Alarm.Set Alarm Status**

Procedure

1 Locate the triggered alarm in the Triggered Alarms panel or on the **Alarms** tab for the object.

2 Right-click the alarm and select **Reset Alarm to Green**.

Identify Disabled Alarm Actions

If you are experiencing problems with alarm actions for a specific inventory object, ensure that alarm actions are enabled for that object.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select a parent object, depending on the scope of objects you want to examine.

- vCenter Server
- Datacenter
- Cluster
- Host
- Virtual Switch
- Datastore Cluster

2 Select the tab that corresponds to the child objects you want to examine.

For example, if the selected inventory object is a datacenter, you might select the Hosts tab.

3 Locate the **Alarm Actions** column.

You might need to scroll horizontally to bring the column into view.

The value in the **Alarm Actions** column indicates whether alarm actions are enabled or disabled on the listed objects.

Viewing Solutions

You can deploy, monitor, and interact with solutions that are installed in a vCenter Server instance with the vCenter Solutions Manager. The Solutions Manager displays information about the health of a solution.

You can navigate to the Solutions Manager from the home page of the vSphere Client. The Solutions Manager view displays information about the solution:

- Solution name
- Solution health
- vService providers

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Click the Solutions Manager icon from vSphere Client home.

2 Navigate through the tabs in the Solutions Manager.

- **Summary** tab. Lists the number of installed solutions and a brief health overview for each of the solutions.

- **Solutions** tab. Lists each managed solution.
- **Health** tab. Provides the health status of the vCenter services. It also shows alerts or warnings for each of the services.

3 In the Solutions Manager inventory, click one of the solutions.

- **Summary** tab. Lists information about the solution, including a link to the product and vendor Web sites, a link to launch the management UI in a separate window, and a link to the virtual machine or vApp running this solution.

  Selecting the vendor Web site link takes you to the Summary page of the virtual machine or vApp. A link under "Managed by" returns you to the solution.
- **Virtual Machines** tab. Lists all the virtual machines belonging to the solution
- **vServices Providers** tab.
- **Management** tab or any other tabs the solution specified.

Configure SNMP Settings for vCenter Server

To use SNMP with vCenter Server, you must configure SNMP settings.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

To complete the following task, the vSphere Client must be connected to a vCenter Server. In addition, you need the DNS name and IP address of the SNMP receiver, the port number of the receiver, and the community identifier.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 If the vCenter Server is part of a linked mode group, in **Current vCenter Server**, select the appropriate server.

3 Click **SNMP** in the navigation list.

4 Enter the following information for the **Primary Receiver** of the SNMP traps.

Option	Description
Receiver URL	The DNS name or IP address of the SNMP receiver.
Receiver port	The port number of the receiver to which the SNMP agent sends traps. If the port value is empty, vCenter Server uses the default port, **162**.
Community	The community identifier.

5 (Optional) Enable additional receivers in the **Enable Receiver 2**, **Enable Receiver 3**, and **Enable Receiver 4** options.

6 Click **OK**.

The vCenter Server system is now ready to send traps to the management system you have specified.

What to do next

Configure your SNMP management software to receive and interpret data from the vCenter Server SNMP agent. See the *vSphere Monitoring and Performance* publication for more information.

System Log Files

In addition to lists of events and alarms, vSphere components generate assorted logs.

These logs contain additional information about activities in your vSphere environment.

View System Log Entries

You can view system logs generated by vSphere components.

Procedure

1 From the Home page of a vSphere Client connected to either a vCenter Server system or an ESX/ESXi host, click **System Logs**.

2 From the drop-down menu, select the log and entry you want to view.

3 Select **View > Filtering** to refer to the filtering options.

4 Enter text in the data field.

5 Click **Clear** to empty the data field.

View System Logs on an ESXi Host

You can use the direct console interface to view the system logs on an ESXi host. These logs provide information about system operational events.

Procedure

1 From the direct console, select **View System Logs**.

2 Press a corresponding number key to view a log.

   vCenter Server agent (vpxa) logs appear if the host is managed by vCenter Server.

3 Press Enter or the spacebar to scroll through the messages.

4 (Optional) Perform a regular expression search.

   a Press the slash key (/).

   b Type the text to find.

   c Press Enter

      The found text is highlighted on the screen.

5 Press q to return to the direct console.

External System Logs

VMware technical support might request several files to help resolve any issues you have with the product. This section describes the types and locations of log files found on various ESXi component systems.

Note On Windows systems, several log files are stored in the Local Settings directory, which is located at `C:\Documents and Settings\<user name>\Local Settings\`. This folder is hidden by default.

ESXi System Logs

You might need the ESXi system log files to resolve technical issues.

The ESXi system logs can be found in the `/var/run/log` directory.

vSphere Client System Logs

You might need the vSphere Client system log files to resolve technical issues.

Table 28-6 lists log files associated with the vSphere Client machine.

Table 28-6. vSphere Client System Logs

Component	Location
vSphere Client Installation log	Temp directory on the vSphere Client machine. Pre-Windows 2008 example: `C:\Documents and Settings\Local Settings\Temp\vminst.log` or `vim-vic-msi.log` Windows 2008 and Windows 7 example: `C:\Users\`*`user_name`*`\AppData\Local\Temp\vminst.log` or `vim-vic-msi.log`
vSphere Client Service log	`\vpx` directory in the Application Data directory on the vSphere Client machine. Pre-Windows 2008 example: `C:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\VMware\vpx\viclient-x.log` Windows 2008 and Window 7 example: `C:\Users\`*`user_name`*`\Local Settings\AppData\Local\VMware\vpx\viclient-x.log` `x(=0, 1, ... 9)`

Export System Logs

When the vSphere Client is connected to vCenter Server, you can select hosts from which to download system logs.

To save diagnostic data for ESX/ESXi hosts and vCenter Server, the vSphere Client must be connected to the vCenter Server system. If you are connected directly to an ESX/ESXi host, you can save diagnostic data only for that specific ESX/ESXi host.

Required privileges:

- To view diagnostic data: **Read-Only User**
- To manage diagnostic data: **Global.Licenses**

Procedure

1. Select **File > Export > Export System Logs**.
2. If you are connected to vCenter Server, select the object for which you want to export data.

   Selecting an object selects all of its child objects.
3. If you are connected to vCenter Server, select **Include information from vCenter Server and vSphere Client** to download vCenter Server and vSphere Client logs as well as host logs.
4. Click **Browse**, and specify the location to which to save the log files.

   The host or vCenter Server generates `.zip` bundles containing the log files. The **Recent Tasks** panel shows a task called "Generate diagnostic bundles" in progress.

   The Downloading Log Bundles dialog box appears when the Generating Diagnostic Bundle task is finished. The download status of each bundle appears in the dialog box.

   Some network errors can cause download failures. When you select an individual download in the upper part of the dialog box, any the error message for that operation appears in the lower portion of the dialog box, below the name and location of the log bundle file.
5. If the download fails, click **Retry** to attempt to download the generated bundles again.

Diagnostic bundles containing log files for the specified objects are downloaded to the location specified.

Configure Syslog on ESXi Hosts

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

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

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

Procedure

1 In the vSphere Client inventory, select the host.

2 Click the **Configuration** tab.

3 In the Software panel, click **Advanced Settings**.

4 Select **Syslog** in the tree control.

5 To set up logging globally, click **global** and make changes to the fields on the right.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified 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.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

6 (Optional) To overwrite the default log size and log rotation for any of the logs.

   a Click **loggers**.

   b Click the name of the log you that want to customize and enter the number of rotations and log size you want.

7 Click **OK**.

Changes to the syslog options take effect immediately.

Collecting Log Files

VMware technical support might request several files to help resolve technical issues. The following sections describe script processes for generating and collecting some of these files.

Set Verbose Logging

You can specify how verbose log files will be.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 Select **Logging Options**.

3 Select **Verbose** from the pop-up menu.

4 Click **OK**.

Collect vSphere Log Files

You can collect vSphere log files into a single location.

Prerequisites

Launch the vSphere Client and log in to a vCenter Server system.

Procedure

◆ View the log file using one of the following methods.

Task	Action
View the `viclient-*.log` file	Change to the directory, `%temp%`.
Download the log bundle from vSphere Client connected to a vCenter Server system	Select **Administration > Export System Logs** to download the log bundle. The log bundle is generated as a `.zip` file. By default, the vpxd logs within the bundle are compressed as `.gz` files. You must use `gunzip` to uncompress these files.
Generate vCenter Server log bundles from a vCenter Server system	Select **Start > Programs > VMware > Generate vCenter Server log bundle**. You can use this to generate vCenter Server log bundles even when you are unable to connect to the vCenter Server using the vSphere Client. The log bundle is generated as a `.zip` file. By default, the vpxd logs within the bundle are compressed as `.gz` files. You must use `gunzip` to uncompress these files.

Collect ESXi Log Files

You can collect and package all relevant ESXi system and configuration information, a well as ESXi log files. This information can be used to analyze the problems.

Procedure

◆ Run the following script on the ESXi Shell: `/usr/bin/vm-support`

The resulting file has the following format: `esx-`*`date-unique-xnumber`*`.tgz`

Turn Off Compression for vpxd Log Files

By default, vCenter Server `vpxd` log files are rolled up and compressed into `.gz` files. You can turn off this setting to leave the `vpxd` logs uncompressed.

Procedure

1 Log in to the vCenter Server using the vSphere Client.

2 Select **Administration > vCenter Server Settings**.

3 Select **Advanced Settings**.

4 In the **Key** text box, type **`log.compressOnRoll`**.

5 In the **Value** text box, type **`false`**.

6 Click **Add**, and click **OK**.

Index

Numerics

3DNow!, EVC modes **131**

A

acceleration, disabling **183**
active adapters **230**
Active Directory
  configuring settings **28**
  server **28**
Active Directory Timeout **78**
active sessions, send messages **22**
active uplinks **262, 265**
adapters
  Ethernet, *See* network adapters
  See also storage controllers
adding
  distributed port groups **43, 236**
  license keys **48, 49**
  NFS storage **324**
  paravirtual SCSI controller **166**
  SCSI controllers **165**
  SCSI devices **170**
  USB controllers **174**
  USB devices to client computers **178**
  vSphere distributed switch **230**
adding a VMkernel network adapter **227**
adding hosts **37**
adjust MAC address allocation parameters **296**
admin contact info **41, 234**
Administrator role **73**
admission control
  configuring **386**
  policy **386**
advanced attributes
  hosts **381**
  Storage I/O Control **352**
  virtual machines **381**
advanced charts, set as default **404**
advanced search **18**
advanced settings
  vCenter Server **32**
  Disk.EnableNaviReg **304**
  Disk.MaxLUN **322**
affinity rules
  creating **366, 367**
  intra-VM **377**
  Storage DRS **375**
agent manager **208**
AHCI SATA controller, *See* storage controllers
alarm actions
  described **408**
  disabling **421**
  email notifications **417**
  notification traps **415**
  running a script **415**
  setting up **415**
alarm environment variables **420**
alarms
  acknowledging triggered alarms **421**
  commands **418**
  condition or state-based **413**
  create **411**
  definitions **411**
  described **408**
  disabling actions **421**
  frequency **414**
  general settings **412**
  network **417, 418**
  notification emails **415**
  reporting settings **414**
  resetting triggered event alarms **421**
  scripts **418, 419**
  send email as alarm action **416**
  set on inventory object **411**
  SMTP settings **416**
  SNMP traps **417, 418**
  trigger tolerance limits **414**
  triggered **411**
  triggers **413**
  viewing **411**
alarms environment variables **419**
alarms,disabled actions **422**
alarms,environment variables **418**
alarms,triggers **414**
alarms,view settings **412**
allowed IP addresses, firewall **60**
AMD Opteron-based systems **379**
AMD override mask **148**
annotations **18**

answer file, update **222**
applying networking policies **257**
assigning license keys **46, 48**
attributes, custom **19**
authentication
  ESXi **69**
  ESXi users **69**
  users **69**
authentication proxy **76, 77**
Auto Deploy **222**
automatic host registration, disabling **304**
automation level
  datastore clusters **369**
  Storage DRS **373**
  virtual machines **358**
average bandwidth **273–276, 279**

B

bandwidth
  average **273, 274**
  peak **273, 274**
Baseboard Management Controller (BMC) **363**
beacon probing, standard switches **260**
best practices, Fault Tolerance **400**
binding on host, distributed port groups **44, 237**
BIOS, settings **182**
blocked ports
  distributed ports **279**
  distributed port groups **279**
boot options
  changing BIOS settings **182**
  changing delay **182**
burst size **273–276, 279**

C

cable/interconnect, health monitoring **406**
CAM server **77**
CDP **293, 295**
CHAP
  disabling **320**
  for discovery targets **319**
  for iSCSI initiators **318**
  for static targets **319**
CHAP authentication **317**
charts
  adding custom to Switch to menu **405**
  advanced **403**
  customizing **403, 404**
  exporting data **406**
  saving data to a file **405**
  settings **404**
  viewing **403**
Cisco Discovery Protocol **41, 234, 294, 295**
Cisco switches **293**
claim rules **333**
client startup options, setting **60**
clones **97**
cloning
  templates **100, 102**
  vApps **198**
  virtual machines **97, 101**
cluster settings
  affinity rules **366, 367**
  CPUID details **132**
  virtual machine swapfile location **347**
clustering, datastores **368, 371**
clusters
  creating **38**
  EVC **128, 129**
  managing profiles from **220**
  removing hosts **80**
  selecting **87**
cold migration **123**
Collection Intervals **27**
commands, alarms **418**
community string **29**
compliance check, Fault Tolerance **395**
compliance checks, host profiles **217**
computer names, generating with a script **110**
config reset at disconnect, distributed port groups **44, 237**
configuration file parameters, editing **141**
configuring
  dynamic discovery **316**
  hosts **23**
  static discovery **317**
consoles, virtual machines **15**
controllers
  paravirtual SCSI **166**
  SCSI **92**
  SCSI types **165**
  See also storage controllers
converting, virtual machines to templates **100**
copy and paste, disabled for guest operating systems **64**
CPU
  health monitoring **406**
  managing allocation **342**
  virtual **379**
CPU affinity, NUMA nodes **379**
CPU compatibility, for vMotion **128**
CPU features, virtual machines **130**
CPUID, viewing details **132**
CPUs
  adding **90**
  advanced settings **147**
  configuration **144**
  defined **143**
  disabling security **148**

enabling CPU/MMU Virtualization **149**
hot adding **144**
hot plug **144**
hyperthreaded core sharing **147**
identification mask **148**
limits **146**
parameters **143**
reservation **146**
scheduling affinity **147**
shares **146**
create alarms **411**
creating
clusters **38**
datastores **39**
host profiles **212, 213**
resource pools **38**
vApps **196**
virtual machines **85**
creating a vSphere HA cluster **384**
creating datacenter-wide networks **40**
creating datacenters **36**
creating host-wide networks **40**
current multipathing state **334**
custom attributes, adding **19**
custom automation mode, DRS **358**
custom sysprep answer file **118**
customization
changing specifications **119**
copying specifications **120**
creating Linux specifications **115**
creating Windows specification **118**
creating Windows specifications **116**
exporting specifications **120**
guest operating system requirements **109**
importing specifications **121**
Linux **109**
Windows **109**
customization specifications **115**

D

database
configuring number of connections **31**
limiting size **31**
retention policy **31**
datacenters
creating **36**
creating datacenter-wide networks **40**
topology maps **83**
datastore clusters
about **368**
adding datastores **371**
automation level **369**
creating **368–370**
maintenance mode **371**
removing datastores **371**
datastores
adding extents **328**
configuring on NFS volumes **324**
creating **39**
grouping **330**
increasing capacity **328**
ISO file **169**
maintenance mode **371**
managing duplicate **324**
mounting **325**
NFS **322**
paths **334**
renaming **329**
review properties **301**
selecting **88**
VMFS **92, 322**
debugging and statistics **183**
default gateway, editing **243**
delete resource pool, vSphere distributed switch **249**
deleting, templates **106**
dependent iSCSI, networking **310**
dependent hardware iSCSI
and associated NICs **308**
configuration workflow **306**
deploying, OVF templates **133**
device disconnection, preventing **65**
DHCP settings **204**
diagnostic partition, configuring **330**
diagnostic bundles, generating **425**
diagnostic data
creating report **425**
export **424**
exporting **425**
direct access **69**
direct console, redirecting to a serial port **23**
directory server, viewing **77**
directory service
Active Directory **76**
configuring a host **76**
DirectPath I/O, vMotion **253**
DirectPath I/O Gen. 2 **253**
disabling
Fault Tolerance **397**
logging for guest operating systems **65**
variable information size **64**
disabling paths **335**
discovery
address **316**
dynamic **316**
static **317**

Disk.EnableNaviReg **304**
Disk.MaxLUN **322**
disks
  format **337**
  independent **190**
  inflate **337**
  limits **162**
  modes **161**
  shares **162**
  thick **101**
  thin **101**
  think vs. thick **102**
distributed ports
  blocked ports **279**
  blocking **279**
  failback **265**
  failover order **265**
  load balancing **265**
  monitoring **238**
  NetFlow **278**
  network failover detection **265**
  Network I/O Control **277**
  network resource pools **277**
  notify switches **265**
  port policies **279**
  properties **238**
  states **238**
  teaming and failover policies **265**
  traffic shaping policies **276**
  VLAN policies **267**
distributed port groups
  adding **43, 236**
  average bandwidth **275, 279**
  binding on host **44, 237**
  blocked ports **279**
  burst size **275, 279**
  config reset at disconnect **44, 237**
  description **43, 237**
  failover order **264, 279**
  failover policies **264, 279**
  forged transmits **271, 279**
  live port moving **44, 237**
  load balancing **264, 279**
  MAC address changes **271, 279**
  miscellaneous policies **279**
  name **43, 237**
  NetFlow **278, 279**
  Network I/O Control **277, 279**
  network resource pools **277, 279**
  notify switches **264, 279**
  number of ports **43, 237**
  override settings **44, 237**
  peak bandwidth **275, 279**
  port policies **279**
  port group type **43, 237**
  port name format **44, 237**
  promiscuous mode **271, 279**
  PVLAN **267, 279**
  QOS policies **267, 279**
  resource pool **248**
  security policy **271, 279**
  teaming policies **264, 279**
  traffic shaping **275, 279**
  virtual machines **246**
  VLAN policy **267, 279**
  VLAN trunking **267, 279**
distributed switch
  adding **230**
  adding a host to **42, 232**
  admin contact info **41, 234**
  Cisco Discovery Protocol **41, 234**
  hosts **233**
  IP address **41, 234**
  jumbo frames **251**
  maximum MTU **41, 234**
  maximum number of ports **41, 234**
  migrating virtual machines to or from **245**
  new resource pool **247**
  ports **233**
  resource pool settings **247**
  upgrading **235**
  virtual machines **245**
  virtual network adapter **243**
  virtual network adapters **241**
DNS **295**
DNS configuration
  vApps **205**
  vSphere distributed switch **243**
DNS lookup **383**
downloading, diagnostic bundles **425**
DPM **356, 362, 363**
DRS
  creating rules **366**
  disabling **359**
  fully automated **357**
  initial placement **356**
  load balancing **356**
  manual **357**
  migration **356**
  partially automated **357**
DRS groups
  host **365**
  virtual machine **366**

DRS clusters
adding managed hosts **359**
adding unmanaged hosts **360**
creating **357**
managing resources with **356**
DVD/CD-ROM, adding **167**
dynamic discovery, configuring **316**
dynamic discovery addresses **316**

E

early binding port groups **43, 237**
editing
host profile policies **215**
host profiles **214**
vApp properties **200, 201**
EFI
changing boot delay **182**
settings **182**
email, content of vCenter Server notifications **417**
Email messages **29**
enabling, host profile policy compliance checks **217**
Enhanced vMotion Compatibility, *See* EVC
Enhanced vMotion Compatibility (EVC) **357**
enhanced vmxnet **250, 251**
entering maintenance mode, host **361**
environment variables, alarms **418, 419**
error messages
Fault Tolerance **391**
vSphere HA **383**
errors, Fault Tolerance **401**
EST **286**
ESX Agent Manager **208**
ESXi
adding users **70**
authentication **69**
rebooting **32**
shutdown **32**
syslog service **24, 66, 426**
users **69**
ESXi Shell
configuring **61**
enabling **61**
enabling with vSphere Client **61**
setting availability timeout **61**
setting idle timeout **61**
timeouts **62**
EVC
configuring **130**
CPUID details **132**
creating a cluster **128**
enabling on a cluster **129**
virtual ESXi host support **128**
EVC modes
virtual machines **130**
without 3DNow! **131**
events
configuring retention policy **31**
exporting **410**
viewing **410**
events,described **408**
export license data **49**
exporting
diagnostic data **425**
host profiles **213**
host users **71**
lists **16**
OVF templates **133, 134**
virtual machines **134**
Extensible Firmware Interface, *See* EFI
extensions, troubleshooting **21**
extents
adding to datastore **328**
growing **328**
External Switch Tagging **286**

F

failback **262, 264, 265, 279**
failover **257, 259, 333**
failover order, distributed port groups **264, 279**
failover policies
distributed ports **265**
distributed port groups **264, 279**
port group **262**
standard switches **260**
fans, monitoring **406**
Fault Tolerance
best practices **400**
checklist **392**
compliance check **395**
disabling **397**
enabling **393**
error messages **391**
errors **401**
Log Bandwidth **398**
logging **243, 393, 394**
migrate secondary **397**
networking configuration **393, 394**
options **396**
prerequisites **392**
secondary location **398**
test failover **397**
test restart secondary **398**
Total Secondary CPU **398**
Total Secondary Memory **398**
turning off **396**

turning on **396**
use cases **391**
version **392**
vLockstep Interval **398**
vSphere configuration **392**
Fault Tolerance status
Disabled **398**
Need Secondary VM **398**
Starting **398**
VM not Running **398**
Fibre Channel NPIV settings **159**
filtering, lists **16**
firewall, configure communication **32**
firewall settings **60**
firewalls
access for management agents **59**
access for services **59**
Flash Read Cache **160**
floppy drives
adding **169**
configuring **170**
forced transmits **272**
forged transmits **269, 271, 279**
fully automated DRS **357**

G

Getting Started tabs
disabling **15**
restoring **15**
grafted, resource pool **359, 360**
groups
DRS host **365**
DRS virtual machine **366**
searching **78**
guest customization
changing specifications **119**
copying specifications **120**
creating Linux specifications **115**
creating Windows specifications **116, 118**
exporting specifications **120**
importing specifications **121**
Linux customization during cloning or deployment **113**
removing specifications **120**
requirements **109**
scripts **110**
specifications **115**
Windows customization during cloning or deployment **111**
guest operating system,remove NIC **241**
guest operating systems
changing **142**
customization requirements **109**
disabling logging **65**
enabling copy and paste **64**
limiting variable information size **64**
selecting **89**

H

hardware, virtual machine **137**
hardware acceleration
about **335**
enabling **336**
hardware devices, SCSI controllers **165**
hardware health, reset sensors **408**
hardware iSCSI initiators
configuring **305**
installing **305**
setting up discovery addresses **316**
viewing **305**
Hardware Virtualization (HV) **392**
health status, monitoring **407**
host
entering maintenance mode **361**
reference **219**
host monitoring, enabling **386**
host registration, disabling **304**
host cache configuration **348**
host configuration, advanced settings **304**
host DRS groups **365**
host health, reset sensors **408**
host image profile acceptance level **25**
host isolation response **387**
Host Limitations, vSphere Client **23**
host name, configuring **76**
host networking, viewing **226**
host power management, custom policy **344**
host profile
attaching entities **217**
SR-IOV **254, 255**
host profiles
accessing **212**
applying profiles **218, 219**
attaching entities from host **218**
attaching entities from Host Profile view **217**
checking compliance **220, 221**
creating **212**
creating from host **213**
creating from host profile view **213**
editing a policy **215**
editing profiles **214**
enabling policy compliance checks **217**
exporting **213**
importing profiles **214**
managing profiles **217**
updating from reference host **220**
usage model **211**

host profiles, cloning profiles **214**
host profiles,import answer file **223**
host security, virtual disk shrinking **63**
host-local swap
  DRS cluster **345**
  standalone host **346**
hosts
  adding **37**
  adding ESXi users **70**
  adding to a vSphere distributed switch **42, 232**
  adding to DRS clusters **359, 360**
  advanced attributes **381**
  clustering **87**
  configuring **23**
  connecting to vCenter Server **79**
  connecting virtual machines to **87**
  custom attributes **18**
  disconnecting **79**
  disconnecting from vCenter Server **79**
  ESXi **32**
  hardware monitoring **406**
  health status **407**
  managing **79**
  reconnecting **80**
  removing from a DRS cluster **362**
  removing from cluster **80**
  removing from vCenter Server **81**
  viable for migration **148**
  virtual machine swapfile location **346**
hot add enablement **144, 151**
hyperthreaded core sharing **147**
hyperthreading
  disabling **343**
  enabling **343**
  server configuration for **343**
hyperthreading modes **343**

I

idle session timeout **62**
iLO, configuring **363**
image files, ISO **168, 169**
importing host profile **214**
inbound traffic shaping **276**
independent disks **190**
independent hardware iSCSI adapters
  change IP address **306**
  change name **306**
information panels **17**
initial placement **356**
installing, plug-ins **20**
Intelligent Platform Management Interface (IPMI), configuring **363**
inter-VM anti-affinity rules, creating **376**
Internet Protocol version 6 **285**
intra-VM anti-affinity rules **377**
inventory
  organize **35**
  searching **17**
  selecting objects **20**
  topology maps **83**
inventory objects, set alarm on **411**
inventory panels **17**
IOMMU **254**
IP address
  editing **243**
  vCenter Server **28**
IP address configuration **204**
IP addresses
  adding allowed **60**
  generating with a script **110**
IP pools **204**
IP storage port groups, creating **227, 242**
IPv4 **383**
IPv6 **285, 383, 393**
iSCSI initiators
  configuring CHAP **318**
  configuring advanced parameters **320**
  hardware **305**
  setting up CHAP parameters **317**
iSCSI networking
  binding adapters **314**
  changing policy **314**
  creating a VMkernel interface **312**
iSCSI SAN **392**
ISO image files **168, 169**
ISO images **400**
isolation response, host **387**

J

jumbo frames
  enabling **251**
  enabling for dependent hardware iSCSI **315**
  enabling for software iSCSI **315**
  using with iSCSI **315**
  virtual machines **250, 251**

L

late binding port groups **43, 237**
Layer 2 security **269**
Layer 2 security policy **269**
License management **45, 47**
license key **45**
License key **47**
license report, export data **49**

licenses
  assigning **46**
  viewing **47**
licensing
  adding license keys **48, 49**
  assigning **48**
  per-processor **48**
licensing limitations, vSphere Client **45**
limiting users or groups **28**
Link Layer Discovery Protocol **293–295**
link status, standard switches **260**
Linux
  customizing during cloning or deployment **113**
  guest operating system customization **109**
  requirements for customization **109**
lists
  exporting **16**
  filtering **16**
live port moving, distributed port groups **44, 237**
LLDP, enable **294**
load balancing
  datastores **368**
  distributed port groups **264, 279**
load balancing policies, standard switches **260**
lockdown mode
  enabling **62**
  vSphere Client **62**
log detail, setting the log level **30**
log files
  collecting **427**
  ESXi **427**
  export **424**
  external **424**
  turning off compression **428**
logging
  disabling for guest operating systems **65**
  enabling **182**
Logging options, configuring **30**
logging in, vSphere Client **14**
logging out, vSphere Client **14**
logical processors **343**
logs
  collecting **427**
  ESXi **424**
  vSphere Client **425**
logs,system, *See also* troubleshooting
Long operations **30**
LUNs, changing number scanned **322**

M

MAC address
  adjust allocation parameters **296**
  configuration **297**
  configuring **296**
  generation **296**
  prefix-based allocation **296**
  range-based allocation **296**
  static **297**
MAC address changes **269, 271, 279**
MAC addresses, assigning **153**
Mail Sender settings, configuring **29**
maintenance mode
  datastores **371, 372**
  hosts **361**
  hosts entering **361**
  ignore affinity rules **372**
management access, firewalls **59**
management interface, securing **59**
management network **383**
managing, virtual machines **185**
Managing **299**
manual DRS **357**
maps **83**
mask values **148**
maximum MTU **41, 234**
maximum number of ports **41, 234**
memory
  affinity **151**
  allocation **150**
  calculating for video displays **171**
  health monitoring **406**
  hot adding **151**
  managing allocation **345**
  virtual **90**
memory affinity, NUMA nodes **380**
memory compression cache
  disabling **348**
  enabling **348**
  set size **349**
migrate secondary, Fault Tolerance **397**
migrating
  powered-off virtual machines **126**
  powered-on virtual machines **124**
  suspended virtual machines **126**
  virtual machine disks **125**
  virtual machines **123**
  virtual machines with Storage vMotion **125**
  with vMotion **124**
migration, about **123**
miscellaneous policies, distributed port groups **279**
modifying cluster settings **384**
monitoring
  Storage I/O Control **350**
  vSphere Client **403**
MTU **250**
multipathing plug-ins, path claiming **333**
multipathing state **334**

multiple monitors, selecting **171**

N

name-ip-generator **110**
NetFlow
  collector settings **293**
  configure **293**
  disable **278, 279**
  distributed ports **278**
  distributed port Groups **278, 279**
  enable **278, 279**
network, SNMP traps **417, 418**
network adapters
  distributed switch **241**
  viewing **226, 235**
  See also NICs
network association settings **205**
network connections, create **312**
network failover detection **262, 265**
Network I/O Control **277**
network partition **400**
network resource management **247**
network resource pools
  distributed ports **277**
  distributed port groups **277, 279**
networking
  advanced **285**
  security policies **272**
networking limitations, vSphere Client **225**
networking policies
  distributed switch **257**
  standard switch **257**
networking configuration, Fault Tolerance **393, 394**
networks
  connecting **91**
  DHCP settings **204**
  health monitoring **406**
  IP address configuration **204**
  proxy server settings **205**
  resource pools **247**
  resource settings **247–249**
new resource pool, distributed switch **247**
New Virtual Machine wizard, opening **85**
NFS storage, adding **324**
NIC teaming, standard switches **260**
NICs
  adding to a vSphere distributed switch **240**
  assigning MAC addresses **153**
  configuring **153**
  guest operating system **241**
  mapping to VMkernel **313**
  remove from a vSphere distributed switch **241**
  remove from active virtual machine **241**
  removing from a vSphere distributed switch **241**
  Spanning Tree protocol **91**
NMP, path claiming **333**
No Access role **73**
Normal operations **30**
notification emails, alarms **415**
notification traps, alarms **415**
notifications, *See* traps
notify switches **262, 264, 265, 279**
NPIV
  assigning WWNs **301**
  changing WWNs **302**
NTP **76**
NUMA
  CPU affinity **379, 380**
  memory affinity **380**
  virtual **379**
NX flag **148**

O

objects, selecting **20**
On-Demand Fault Tolerance **391**
optical drives
  connecting to client device **168**
  connecting to host device **168**
outbound traffic shaping **276**
OVA, selecting, *See also* OVF
override settings, distributed port groups **44, 237**
OVF
  defining environment properties **203**
  deploying templates **133**
  exporting templates **133, 134**
  folder location for files **134**

P

panels **17**
parallel ports
  adding **158**
  changing **159**
paravirtual SCSI controller **166**
parent resource pool **352**
partially automated DRS **357**
passthrough device, add to a virtual machine **253**
path claiming **333**
path failover **333**
path management **333**
path policies, changing defaults **335**
paths, disabling **335**
PCI **252**
PCI devices, snapshot support for **171**
PCIe devices **254**

peak bandwidth **273–276, 279**
per-processor licensing **48**
performance, advanced charts **403**
performance charts
advanced charts
about **403**
deleting views **405**
customizing **404**
exporting data **406**
saving data to a file **405**
permissions
administrator **72**
and privileges **72**
changing **72**
overview **72**
removing **73**
root user **72**
search **17**
validating **72, 73**
vpxuser **72**
physical compatibility mode **95**
physical network adapters
adding to a vSphere distributed switch **240**
managing **240**
removing **241**
physical processors **343**
planning a vSphere HA cluster **383**
plug-ins
disabling **20**
downloading **20**
enabling **20**
installing **20**
managing **20**
removing **21**
troubleshooting **21**
viewing installed **20**
policies, CPU power management **344**
port blocking **257**
port configuration **229**
port groups
failback **262**
failover order **262**
Layer 2 Security **270**
load balancing **262**
network failover detection **262**
notify switches **262**
traffic shaping **274**
port mirroring
create **289**
destinations **290–292**
feature compatibility **287**
LRO **287**
name **289, 291**
packet length **289**
session types **287**
sources **290–292**
status **291**
TSO **287**
verify settings **290**
version compatibility **287**
VLAN **289, 291**
vMotion **287**
port name format, distributed port groups **44, 237**
port policies, distributed port groups **279**
ports
adding parallel **158**
changing parallel **159**
changing serial **157**
parallel **154**
serial **154**
vSphere distributed switch **41, 234**
power, health monitoring **406**
power management policies, setting **344**
power off
vApps **198**
virtual machines **180**
power on
vApps **197**
virtual machines **180**
power states, virtual machine **180**
prefixed-based MAC address allocation **296**
prerequisites, Fault Tolerance **392**
printing, vSphere Client window **17**
private VLAN
create **239**
primary **239**
removing **239, 240**
secondary **240**
privileges and permissions **72**
processors
health monitoring **406**
See also CPUs
profiles, managing **220**
promiscuous mode **269, 271, 272, 279**
properties, distributed ports **238**
proxy server settings, networks **205**
PVLAN **267**
PVSCSI, *See also* paravirtual SCSI controller

Q

QOS policies, distributed port groups **267, 279**
query limit **28**

R

range-based MAC address allocation **296**
raw device mapping **332**

raw device mappings **92, 95, 160, 161**
RDM **392**
RDMs, path management **333**
Read Only role **73**
receiver URL **29**
recommendations, Storage DRS **372**
reconnecting hosts **80**
reference host **219**
removing, plug-ins **21**
renaming, templates **105**
rescanning
  datastores **321**
  storage adapters **321**
  storage devices **321**
reset sensors, host health **408**
resetting virtual machines **180**
resignaturing **324**
resource pools
  adding virtual machines **355**
  creating **38, 353**
  deleting **356**
  editing attributes of **355**
  grafted **359, 360**
  networks **247**
  parent **352**
  removing **356**
  removing virtual machines **356**
  root resource pool **352**
  selecting **88**
  siblings **352**
resource allocation settings, changing **342**
resource management
  customizing **381**
  hosts **341**
resource maps
  exporting **84**
  printing **84**
  setting maximum number of map objects **84**
  viewing **84**
resource pool, distributed port groups **248**
resource pool settings
  distributed switch **247**
  vSphere distributed switch **249**
restart settings, for virtual machines **180**
resume
  vApps **199**
  virtual machines **180**
roles
  Administrator **73**
  and permissions **73**
  cloning **74**
  copy **74**
  creating **74**
  default **73**
  editing **74**
  No Access **73**
  Read Only **73**
  removing **73, 75**
  renaming **75**
  security **73**
root login, permissions **72**
root resource pool **352**
routing **295**
Runtime Settings, configuring **28**

S

SAN LUN **95**
SAN LUNs **160, 161**
SATA controllers
  default behavior **163**
  maximum number of **163**
  node assignment **163**
  See also storage controllers
scanning, changing number **322**
scheduled tasks
  about **53**
  about canceling **56**
  canceling **53**
  clone virtual machine **100**
  creating **54**
  process rules **57**
  removing **56**
  rules **57**
scheduling affinity **147**
scratch partition,enabling **24**
scripts, alarms **418, 419**
SCSI
  bus sharing **165**
  changing controller type **165**
  controllers, adding **165**
  devices, adding **170**
  devices, changing **171**
  paravirtual controllers **166**
  selecting controllers **92**
  supported controller types **165**
  VMware Paravirtual **92**
SCSI controllers
  adding **163**
  and virtual device nodes **163**
  default virtual hard disk assignments **163**
  maximum number of **163**
  types **163**
search, advanced **18**
search lists, adjusting for large domains **78**
searching
  inventory objects **17**
  simple search **17**

searching inventory, permissions **17**
security, permissions **72**
security policies, distributed ports **272**
security policy
  distributed port groups **271, 279**
  policy exceptions **269**
  virtual switches **269**
selecting datastores **88**
serial port, redirecting the direct console using the vSphere Client **23**
serial ports
  adding **156**
  adding Firewall rule set **155**
  changing **157**
  conditions for network connections **155**
  conditions for physical connections **154**
  connection types **154**
server configuration for hyperthreading **343**
service startup
  changing policy **60**
  setting options **60**
service startup options, setting **60**
services, syslogd **24, 66, 426**
sessions
  viewing **21**
  vSphere Client, terminating **21**
set host to evaluation mode **46**
settings, vCenter Server **23, 26**
shares, Storage I/O Control **349**
shares and limits, Storage I/O Control **350**
sharing, disks **94**
shutdown, settings for virtual machines **180**
shutdown, settings, for virtual machines **185**
siblings **352**
simple search **17**
Single Root I/O Virtualization **254**
SMASH **406**
SMTP
  configuring **416**
  notification **29**
  server **29**
snapshots
  about **187**
  behavior **187**
  child **187**
  consolidating **194**
  Delete all option **193**
  Delete option **193**
  deleting **193**
  delta disks **187**
  exclude virtual disks from **190**
  GO to command **192**
  hierarchy **187**
  memory **189**
  parent **187**
  quiescing **190**
  quiescing virtual machine files **189**
  restoring **191, 192**
  revert to parent **192**
  reverting to **191**
  taking **189, 190**
  virtual machine activity **189**
  virtual machines with dynamic disks **190**
SNMP
  community string **29**
  configuring **423**
  receiver URL **29**
  settings **29**
  traps **29**
SNMP traps **417, 418**
software iSCSI, networking **310**
software FCoE
  and VMkernel **303**
  activating adapters **304**
software iSCSI initiator, enabling **308**
software iSCSI adapter
  configuring **308**
  disabling **309**
software iSCSI initiators, setting up discovery addresses **316**
solutions,viewing **208, 422**
specify failover hosts **387**
SR-IOV
  enable **254, 255**
  host profile **254, 255**
SSL certificate **80**
standard switch **227**
standard switches
  average bandwidth **274**
  beacon probing **260**
  burst size **274**
  failover **260**
  forged transmits **269**
  link status **260**
  load balancing policies **260**
  MAC address changes **269**
  NIC teaming **260**
  peak bandwidth **274**
  port configuration **229**
  promiscuous mode **269**
  security policy **269**
  traffic shaping policies **274**
standby adapters **230**
standby mode **356, 362, 363**
standby settings, for virtual machines **180**
standby uplinks **262, 265**
starting, vSphere Client **14**

startup settings, for virtual machines **185**
states, distributed ports **238**
static discovery, configuring **317**
static discovery addresses **316**
Statistics, Collection Intervals **27**
status bar **14**
storage
  health monitoring **406**
  iSCSI **392**
  NAS **392**
  NFS **392**
  not-shared **337**
  provisioned **337**
  Storage Limitations, vSphere Client **300**
  used by virtual machines **337**
  vSphere Client, Storage Limitations **300**
storage adapters
  about **306**
  rescanning **321**
  viewing **301**
storage controllers
  AHCI SATA **163**
  and snapshots **163**
  BusLogic Parallel **163**
  compatibility **163**
  IDE **163**
  limitations for VMware Paravirtual SCSI **166**
  limitations of **163**
  LSI Logic SAS **163**
  maximum number of **163**
  SCSI **163**
  VMware Paravirtual SCSI **163, 166**
storage device, renaming **321**
storage filters, disabling **331**
Storage APIs, Storage Awareness **338**
storage devices
  displaying for a host **300**
  displaying for an adapter **301**
  managing **321**
  paths **334**
  rescanning **321**
Storage DRS
  about **369**
  affinity rules **375**
  anti-affinity rules **376**
  automation level **373**
  disabling **369**
  enabling **369**
  maintenance mode **371**
  recommendations **372, 373**
  scheduled task **374**
  statistics **378**
Storage I/O Control
  enabling **351**
  limitations **349**
  monitoring **350**
  requirements **349**
  shares and limits **349–351**
  threshold **352**
Storage vMotion **123**
storing, device nodes, using nondefault device notes **93**
subnet mask, editing **243**
support information **45**
suspending
  vApps **198**
  virtual machines **180**
swap file, deleting **348**
swap file location **152**
swap to SSD **348**
swapfile location **347**
swapfiles **346**
syslog **24, 66, 426**
Sysprep Answer Files
  custom **118**
  sysprep.inf **118**
  sysprep.xml **118**
system logs
  configuring **427**
  downloading **425**
  ESXi **424**
Systems Management Architecture for Server Hardware, *See* SMASH

T

tabs, Getting Started **15**
tasks
  about **51**
  canceling **53**
  clone virtual machine **100**
  configuring retention policy **31**
  filtering on hosts and datacenters **52**
  filtering with keywords **53**
  guidelines **57**
  removing scheduled tasks **56**
  rescheduling **56**
  rules **57**
  scheduled, about **53**
  scheduling **54**
  viewing **14, 51**
  viewing all tasks **51**
  viewing recent tasks **52**
  viewing scheduled tasks **52**
teaming policies
  distributed ports **265**

distributed port groups **264, 279**
port group **262**
temperature, monitoring **406**
templates
changing names **105**
cloning **101, 102**
converting to virtual machines **107**
converting virtual machines to **100**
creating **100, 101**
deleting **106**
deploy virtual machines **103**
OVF **134**
removing from inventory **106**
renaming **105**
returning to inventory **107**
returning to a host **187**
unregistering **106**
test failover, Fault Tolerance **397**
test restart secondary, Fault Tolerance **398**
thick provisioned disks **101, 102**
thin disks, creating **336**
thin provisioned disks **101, 102**
thin provisioning **336**
Thin Provisioning **93**
threshold, Storage I/O Control **352**
time zones **56**
timeout, ESXi Shell **62**
Timeout, interval **30**
timeout interval, setting **28**
Timeout settings, configuring **30**
traffic shaping
distributed port groups **275, 279**
port groups **274**
traffic shaping policies
distributed ports **276**
uplink ports **276**
traps, SNMP **417, 418**
triggered alarms, acknowledging **421**
triggers, event-based **414**
troubleshooting
debugging and statistics **183**
extensions **21**
log files **424, 427**
plug-ins **21**
virtual machine software installation **183**
TSO **250**
turning off, Fault Tolerance **396**

U

updated information **11**
upgrading
distributed switch **235**
virtual machine hardware **139**
VMware Tools **142**
vSphere distributed switch **235**
uplink adapters
adding **230**
adding to a vSphere distributed switch **240**
duplex **229**
managing **240**
removing **241**
speed **229**
uplink assignments **235**
uplink port groups, VLAN policies **268**
uplink ports
traffic shaping policies **276**
VLAN policies **267, 268**
USB passthrough
arbitrator for **173**
avoiding data loss **177**
configuring from a client computer to a VM **177**
configuring from a host to a virtual machine **173**
controllers for **173, 177**
devices, *See also* USB devices
USB controllers
adding to virtual machine **174**
removing from virtual machine **175**
USB devices
adding from client computer to VM in the vSphere Client **179**
adding host device to virtual machine **176**
adding to client computers **178**
behavior with hot add operations **177**
removing from virtual machine **177**
removing remote client device from VM **179**
supported devices for Mac OS X guest **177**
use cases, Fault Tolerance **391**
user management, ESXi **69**
users
adding to ESXi **70**
authentication **69**
direct access **69**
exporting a user list **71**
modifying on hosts **70**
removing **72**
removing from hosts **71**
searching **78**
security **69**
viewing user list **71**

V

validation
enabling **28**

of users or groups **28**
period **28**
vApps
adding objects to **199**
advanced properties **202**
cloning **198**
configuring DNS **205**
configuring IP address **204**
configuring networks **201**
creating **196**
creating objects inside **199**
defining OVF environment properties **203**
editing advanced IP allocation properties **203**
editing annotations **206**
editing custom properties **203**
editing properties **200, 201**
editing resources **200**
IP pools **204**
managing **195**
populating **199**
power off settings **198**
power on settings **197**
resuming **199**
selecting DHCP **204**
selecting network associations **205**
selecting proxy server for **205**
shutdown options **200**
startup options **200**
suspending **198**
variable information size for guest operating systems
disabling **64**
limiting **64**
vCenter Converter client plug-in **133**
vCenter Server
active sessions, view **21**
advanced settings **32**
assign license **26**
communication through firewall **32**
configuring **26**
configuring SNMP **423**
custom attributes **18**
database connections **31**
ID **28**
IP address **28**
license **26**
licensing **26**
name **28**
SNMP **417**
vCenter Server email agent **417**
vCenter Server limitations, vSphere Client **26**
vendor providers
registering **338**
unregistering **339**
updating **339**
viewing **339**
verbose logging, configuring **427**
version, virtual machine **89**
VGT **286**
video cards
configuring **171**
selecting number of displays **171**
virtual hardware
adding host USB devices to virtual machine **176**
adding USB devices **179**
CPU advanced settings **147**
CPU hyperthreading **147**
CPU/MMU enablement **149**
CPUs **90**
disks **92**
hot add enablement **144**
hot adding virtual CPUs **144**
memory **90**
NICs **91**
parallel ports **158, 159**
SCSI controllers **92**
SCSI devices **170, 171**
serial ports **156**
video cards **171**
Virtual LAN **286**
virtual machine, memory **150**
virtual processors, *See* CPUs
virtual adapter **243**
virtual compatibility mode **95**
virtual CPUs, changing number **379**
virtual device node **171**
virtual devices, adding USB controller **174**
virtual disks
clustering features **93**
configuration **161**
configuring **160**
creating **93**
flat format **93**
modes **93**
requirements for guest operating system customization **109**
sharing **94**
shrinking **63**
sparse **160**
thin provisioning **160**
thin format **93**

types **92**
using nondefault device node **93, 94**
Virtual Guest Tagging **286**
virtual machine hardware
determining version **140**
upgrading **139**
virtual disks **161**
virtual machine affinity **365–367**
virtual machine anti-affinity **365–367**
virtual machine console **186**
virtual machine DRS groups **366**
virtual machine hardware version **139**
Virtual Machine Limitations, vSphere Client **138**
virtual machine monitoring **388**
virtual machine networking **227**
virtual machine options, vSphere HA **387**
virtual machine overrides **389**
Virtual Machine Startup and Shutdown feature **384**
virtual machine swapfile location **347**
virtual machines
acceleration **183**
adding **186**
adding to DRS clusters **360**
adding to resource pools **355**
advanced attributes **381**
assigning to a specific processor **344**
assigning WWNs to **301**
changing name **141**
cloning **97**
completing **96**
configuration file location **141**
configuring **137**
configuring devices **167**
converting templates to **107**
converting to templates **100**
CPU configuration **144**
CPU resources **143**
creating **85, 86**
custom attributes **18**
debugging **183**
deploy from templates **103**
disable copy and paste **64**
disabling logging **65**
DRS automation level **358**
enabling logging **182**
EVC modes **130**
exporting **134**
floppy drives **169, 170**
guest operating system **142**
hard disks **161**
hardware **137**
hardware versions **139**
hardware version **140**
hot add enablement **151**
limiting variable information size **64**
managing **185**
memory **149**
migrating **123, 125, 126**
migrating to or from a distributed switch **245**
migrating to or from a vSphere distributed switch **245**
migration **123**
naming **87**
network adapter **154**
network configuration **153**
networking **245, 246**
NIC **154**
opening console **186**
optical drives **167**
power management settings **180**
power states **180**
preventing device disconnection **65**
remove from a host **186**
remove from the datastore **187**
removing **186**
removing from a DRS cluster **361**
removing from resource pools **356**
resources **137**
restart priority **387**
returning to a host **187**
scheduled task to clone **100**
selecting configuration option for creation **86**
selecting guest operating systems **89**
shutdown settings **185**
snapshots **187**
startup settings **185**
swap file **152**
swapfile location **346, 347**
templates, converting to **100**
upgrading hardware version **139**
versions **89**
view console **15**
Virtual SMP **90**
with RDMs **332**
See also templates, clones
See also virtual hardware
virtual memory
allocation **149**
configuring **149**
virtual network adapters, removing **245**
virtual NUMA **379**
Virtual Serial Port Concentrator **154, 156**

Virtual SMP **90**
Virtual Switch Tagging **286**
VLAN
  port mirroring **289, 291**
  private **239**
VLAN ID
  primary **239**
  secondary **239**
VLAN policies
  distributed ports **267**
  uplink ports **267, 268**
  uplink port groups **268**
VLAN policy, distributed port groups **267, 279**
VLAN trunking, distributed port groups **267, 279**
VLAN Trunking **43, 236, 267**
VLAN Type **267**
VM Component Protection **383**
VM-Host affinity rule **365–367**
VM-VM affinity rule **365, 366**
VMCP **383**
VMDK **392**
VMFS, resignaturing **324**
VMFS datastores
  adding extents **328**
  changing signatures **325**
  creating on Fibre Channel storage **323**
  creating on iSCSI storage **323**
  creating on SCSI disk **323**
  creating on storage device **323**
  deleting **330**
  increasing capacity **328**
  rescanning **321**
  upgrading **326**
VMFS resignaturing **324**
VMFS volume **160**
VMFS2 datastores, upgrading **327**
VMFS3, upgrading **328**
VMkernel
  gateway **229, 244**
  jumbo frames **250**
  prefix **229, 244**
  routing **229, 244**
VMkernel interfaces **313**
VMkernel network adapters
  adding **227, 242**
  editing **243**
  enabling vMotion **243**
  fault tolerance logging **243**
vMotion
  3DNow! **131**
  CD-ROM migration limitation **168**
  compatibility **148, 252**
  compatibility checks **128**
  DirectPath I/O **253**
  enabling on a virtual network adapter **243**
  migrating virtual machines with **124**
  port mirroring **287**
vMotion interfaces, creating **227, 242**
VMware Compatibility Guide, accessing **109**
VMware Paravirtual SCSI controllers **166**
VMware Tools
  requirement for customization **109**
  upgrading **142**
vpxd, log files **428**
vService, add a dependency **172, 201**
vService, edit a dependency **173, 202**
vservices, configuring **172**
vServices, remove dependency **173, 202**
vServices,monitoring **209**
vSPC **154, 156**
vSphere Client, Host Limitations **23**
vSphere Client, networking **225**
vSphere Administration with vSphere Client **9**
vSphere Authentication Proxy **76, 77**
vSphere CLI **24**
vSphere Client
  about **13**
  communication through firewall **32**
  licensing limitations **45**
  logging in **14**
  logging out **14**
  logs **425**
  panels **17**
  printing data **17**
  sessions **21**
  starting **14**
  stop **14**
vSphere Client, networking limitations **225**
vSphere Client, vCenter Server limitations **26**
vSphere Client, Virtual Machine Limitations **138**
vSphere distributed switch
  adding **230**
  adding a host to **42, 232**
  adding a VMkernel network adapter **242**
  admin contact info **41, 234**
  CDP **294**
  Cisco Discovery Protocol **41, 234, 294**
  delete resource pool **249**
  editing **243**
  hosts **233**
  IP address **41, 234**
  jumbo frames **251**
  LLDP **294**
  manage hosts **233**
  maximum MTU **41, 234**

maximum number of ports **41, 234**
migrating virtual machines to or from **245**
mirror **286**
port mirroring **286**
ports **233**
protection against MAC address impersonation **269**
protection against traffic scanning **269**
resource pool settings **249**
security policy **269**
upgrading **235**
virtual machines **245**
virtual network adapter **243**
virtual network adapters **241**
vSphere Distributed Switch
Network I/O Control **247**
See also distributed switch Network I/O Control
vSphere DRS, creating rules **367**
vSphere HA
checklist **383**
cluster settings **384**
configuring cluster settings **386**
error messages **383**
virtual machine monitoring **388**
virtual machine options **387**
vSphere HA cluster
creating **384, 395**
planning **383**
vSphere HA admission control, policy **387**
vSphere HA datastore heartbeating **388**
vSphere standard switch
port configuration **229**
protection against MAC address impersonation **269**
protection against traffic scanning **269**
security policy **269**
teaming and failover policies **262**
viewing **226**
VST **286**

W

wake protocols **363**
Wake-on-LAN (WOL), testing **364**
watchdog, health monitoring **406**
Windows
customizing during cloning or deployment **111**
guest operating system customization **109**
requirements for customization **109**
World Wide Names, *See* WWNs
WWNNs **301**
WWNs
assigning to virtual machines **301**
changing **302**
WWPNs **301**