vSphere Datacenter Administration Guide

ESX 4.1
ESXi 4.1
vCenter Server 4.1

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-000297-02

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

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

Contents

Monitoring Your Virtual Infrastructure

Maintaining Your Virtual Infrastructure

Appendixes

Updated Information

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

This table provides the update history of the *vSphere Datacenter Administration Guide*.

Revision	Description
000297-02	Included a Privilege in "Virtual Machine Provisioning," on page 261
000297-01	Changed a point in "Configuring Communication Among ESX, vCenter Server, and the vSphere Client," on page 57.
000297-00	Initial release.

About This Book

Datacenter Administration Guide describes how to start and stop the VMware® vSphere Client components, build your vSphere environment, monitor and manage the information generated about the components, and set up roles and permissions for users and groups using the vSphere environment.

In addition, this manual provides brief introductions to the various tasks you can perform within the system as well as cross-references to the documentation that describes all the tasks in detail.

Datacenter Administration Guide covers ESX, ESXi, and vCenter Server.

Intended Audience

The information presented is for system administrators who are experienced Windows or Linux system administrators and who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

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

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware vSphere Documentation

The vSphere documentation consists of the combined VMware vCenter Server and ESX/ESXi documentation set.

Abbreviations Used in Figures

The figures in this manual use the abbreviations listed in Table 1.

Table 1. Abbreviations

Abbreviation	Description
database	vCenter Server database
datastore	Storage for the managed host
dsk#	Storage disk for the managed host
hostn	vCenter Server managed hosts

Table 1. Abbreviations (Continued)

Abbreviation	Description
SAN	Storage area network type datastore shared between managed hosts
tmplt	Template
user#	User with access permissions
VC	vCenter Server
VM#	Virtual machines on a managed host

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Virtualization with VMware vSphere

vSphere Concepts and Features 1

VMware vSphere™ leverages the power of virtualization to transform datacenters into simplified cloud computing infrastructures and enables IT organizations to deliver flexible and reliable IT services.

The two core components of vSphere are VMware ESX/ESXi™ and VMware vCenter Server™. ESX/ESXi is the virtualization platform on which you create and run virtual machines. vCenter Server is a service that acts as a central administrator for ESX/ESXi hosts that are connected on a network. vCenter Server allows you to pool and manage the resources of multiple hosts. vCenter Server provides many features that allow you to monitor and manage your physical and virtual infrastructure.

Additional vSphere components are available as plugins that extend the functionality of the vSphere product.

This chapter includes the following topics:

Virtualization Basics

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The hypervisor serves as a platform for running virtual machines and allows for the consolidation of computing resources.

Each virtual machine contains its own virtual, or software-based, hardware, including a virtual CPU, memory, hard disk, and network interface card.

Software called the hypervisor is installed on the physical hardware in a virtualized datacenter, and acts as a platform for virtual machines. ESX/ESXi is the hypervisor in a vSphere environment. The hypervisor provides physical hardware resources dynamically to virtual machines as needed to support the operation of the virtual machines. The hypervisor allows virtual machines to operate with a degree of independence from the underlying physical hardware. For example, a virtual machine can be moved from one physical host to another, or its virtual disks can be moved from one type of storage to another, without affecting the functioning of the virtual machine.

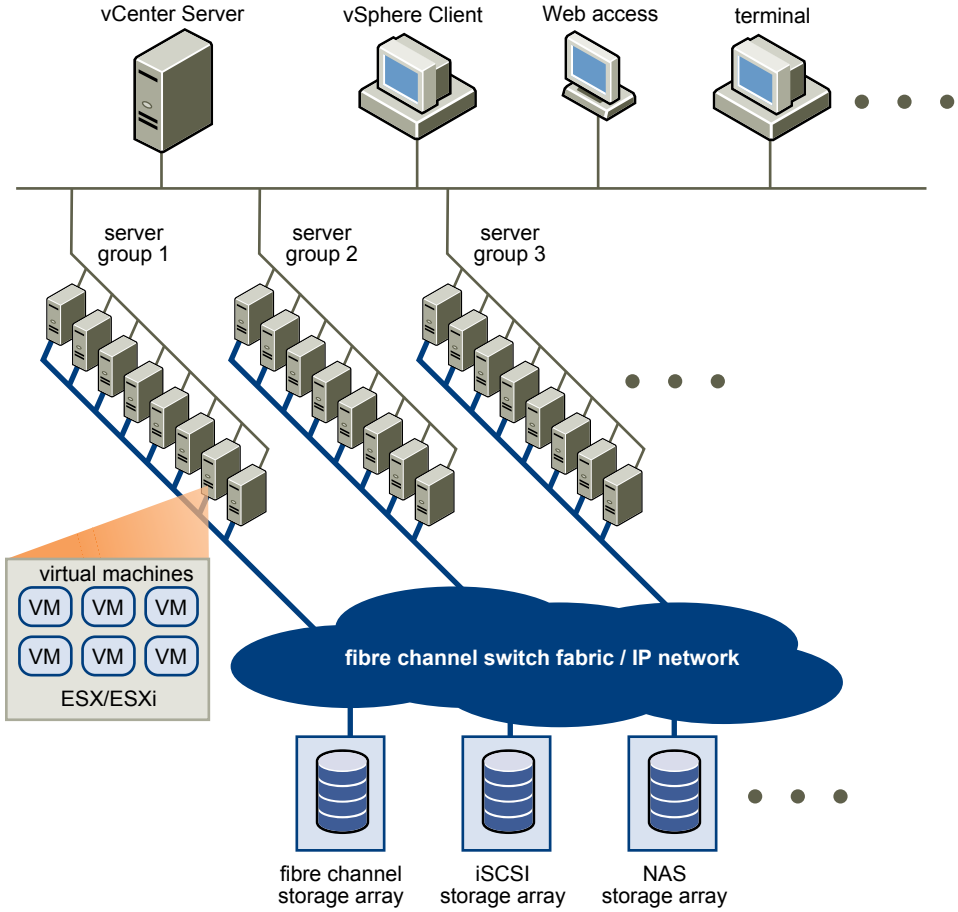
Because virtual machines are decoupled from specific underlying physical hardware, virtualization allows you to consolidate physical computing resources such as CPUs, memory, storage, and networking into pools of resources that can be dynamically and flexibly made available to virtual machines. With appropriate management software, such as vCenter Server, you can also use a number of features that increase the availability and security of your virtual infrastructure.

Physical Topology of vSphere Datacenter

A typical VMware vSphere datacenter consists of basic physical building blocks such as x86 virtualization servers, storage networks and arrays, IP networks, a management server, and desktop clients.

This physical topology of the vSphere datacenter is illustrated in Figure 1-1.

Figure 1-1. VMware vSphere Datacenter Physical Topology



The vSphere datacenter topology includes the following components.

Computing servers Industry standard x86 servers that run ESX/ESXi on the bare metal. ESX/ESXi software provides resources for and runs the virtual machines. Each computing server is referred to as a standalone host in the virtual environment. You can group a number of similarly configured x86 servers with connections to the same network and storage subsystems to provide an aggregate set of resources in the virtual environment, called a cluster.

Storage networks and arrays Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

IP networks Each computing server can have multiple NICs to provide high bandwidth and reliable networking to the entire VMware vSphere datacenter.

vCenter Server vCenter Server provides a single point of control to the datacenter. It provides essential datacenter services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire datacenter. It does this by managing the assignment of virtual machines to the computing servers and the assignment of resources to the virtual machines within a given computing server based on the policies that the system administrator sets.

Computing servers continue to function even in the unlikely event that vCenter Server becomes unreachable (for example, if the network is severed). Servers can be managed separately and continue to run the virtual machines assigned to them based on the resource assignment that was last set. After connection to vCenter Server is restored, it can manage the datacenter as a whole again.

Management clients VMware vSphere provides several interfaces for datacenter management and virtual machine access. These interfaces include VMware vSphere Client (vSphere Client), web access through a web browser, vSphere Command-Line Interface (vSphere CLI), or vSphere Management Assistant (vMA).

vSphere Software Components

VMware vSphere is a suite of software components for virtualization. These include ESX/ESXi, vCenter Server, and other software components that fulfill a number of different functions in the vSphere environment.

vSphere includes the following software components:

ESX/ESXi A virtualization platform that you use to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.

Through ESX/ESXi, you run the virtual machines, install operating systems, run applications, and configure the virtual machines. Configuration includes identifying the virtual machine's resources, such as storage devices.

The server provides bootstrapping, management, and other services that manage your virtual machines.

Each ESX/ESXi host has a vSphere Client available for your management use. If your ESX/ESXi host is registered with vCenter Server, a vSphere Client that accommodates vCenter Server features is available.

vCenter Server

A service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).

vCenter Server is a single Windows Service and is installed to run automatically. vCenter Server runs continuously in the background. It performs its monitoring and managing activities even when no vSphere Clients are connected and when no one is logged on to the computer where it resides. It must have network access to all the hosts it manages and be available for network access from any machine where the vSphere Client is run.

You can install vCenter Server in a Windows virtual machine on an ESX/ESXi host, allowing it to take advantage of the high-availability that is provided by VMware HA. See the *ESX and vCenter Server Installation Guide* for details about setting up this configuration.

You can join multiple vCenter Server systems using Linked Mode to allow them to be managed using a single vSphere Client connection.

vCenter Server plug-ins

Applications that provide additional features and functionality to vCenter Server. Typically, plug-ins consist of a server component and a client component. After the plug-in server is installed, it is registered with vCenter Server and the plug-in client is available to vSphere clients for download. After a plug-in is installed on a vSphere client, it might alter the interface by adding views, tabs, toolbar buttons, or menu options related to the added functionality.

Plug-ins leverage core vCenter Server capabilities, such as authentication and permission management, but can have their own types of events, tasks, metadata, and privileges.

Some vCenter Server features are implemented as plug-ins, and can be managed using the vSphere Client Plug-in Manager. These features include vCenter Storage Monitoring, vCenter Hardware Status, and vCenter Service Status.

vCenter Server database

A persistent storage area for maintaining the status of each virtual machine, host, and user managed in the vCenter Server environment. The vCenter Server database can be remote or local to the vCenter Server system.

The database is installed and configured during vCenter Server installation.

If you are accessing your ESX/ESXi host directly through a vSphere Client, and not through a vCenter Server system and associated vSphere Client, you do not use a vCenter Server database.

Tomcat Web server

Many vCenter Server functions are implemented as Web services that require the Tomcat Web server. The Tomcat Web server is installed on the vCenter Server machine as part of the vCenter Server installation.

Features that require the Tomcat Web server to be running include: Linked Mode, CIM/Hardware Status tab, Performance charts, WebAccess, vCenter Storage Monitoring/Storage Views tab, and vCenter Service status.

vCenter Server agent

On each managed host, the software that collects, communicates, and executes the actions received from vCenter Server. The vCenter Server agent is installed the first time any host is added to the vCenter Server inventory.

Host agent On each managed host, the software that collects, communicates, and executes the actions received through the vSphere Client. It is installed as part of the ESX/ESXi installation.

LDAP vCenter Server uses LDAP (Lightweight Directory Access Protocol) to synchronize data such as license and role information across vCenter Server systems joined in Linked Mode.

vSphere Managed Inventory Objects

In vSphere, the inventory is a collection of virtual and physical objects on which you can place permissions, monitor tasks and events, and set alarms. You can group most inventory objects by using folders to more easily manage them.

All inventory objects, with the exception of hosts, can be renamed to represent their purposes. For example, they can be named after company departments or locations or functions. vCenter Server monitors and manages the following components of your virtual and physical infrastructure:

Clusters A collection of ESX/ESXi hosts and associated virtual machines intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts.

If you enable VMware EVC on a cluster, you can ensure that migrations with vMotion do not fail because of CPU compatibility errors. If you enable VMware DRS on a cluster, the resources of the hosts in the cluster are merged to allow resource balancing for the hosts in the cluster. If you enable VMware HA on a cluster, the resources of the cluster are managed as a pool of capacity to allow rapid recovery from host hardware failures.

Datacenters Unlike a folder, which is used to organize a specific object type, a datacenter is an aggregation of all the different types of objects needed to do work in virtual infrastructure: hosts, virtual machines, networks, and datastores.

Within a datacenter there are four separate hierarchies.

- Virtual machines (and templates)
- Hosts (and clusters)
- Networks
- Datastores

The datacenter defines the namespace for networks and datastores. The names for these objects must be unique within a datacenter. For example, you cannot have two datastores with the same name within a single datacenter, but you can have two datastores with the same name in two different datacenters. Virtual machines, templates, and clusters need not be unique within the datacenter, but must be unique within their folder.

Objects with the same name in two different datacenters are not necessarily the same object. Because of this, moving objects between datacenters can create unpredictable results. For example, a network named networkA in datacenterA might not be the same network as a network named networkA in datacenterB. Moving a virtual machine connected to networkA from datacenterA to datacenterB results in the virtual machine changing the network it is connected to.

Datastores	A virtual representation of underlying physical storage resources in the datacenter. A datastore is the storage location for virtual machine files. These physical storage resources can come from the local SCSI disk of the ESX host, the Fibre Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. Datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines.
Folders	Folders allow you to group objects of the same type so you can easily manage them. For example, you can use folders to set permissions across objects, to set alarms across objects, and to organize objects in a meaningful way. A folder can contain other folders, or a group of objects of the same type: datacenters, clusters, datastores, networks, virtual machines, templates, or hosts. For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines. Datacenter folders form a hierarchy directly under the root vCenter Server and allow users to group their datacenters in any convenient way. Within each datacenter is one hierarchy of folders with virtual machines and templates, one with hosts and clusters, one with datastores, and one with networks.
Hosts	The physical computer on which ESX/ESXi is installed. All virtual machines run on hosts. If the vSphere Client is connected directly to an ESX/ESXi host, only that host is available for management.
Networks	A set of virtual network interface cards (virtual NICs), virtual switches (vSwitches) or vNetwork Distributed Switches, and port groups or dvPort groups that connect virtual machines to each other or to the physical network outside of the virtual datacenter. All virtual machines that connect to the same port group belong to the same network in the virtual environment, even if they are on different physical servers. You can monitor networks and set permissions and alarms on port groups and dvPort groups.
Resource pools	Resource pools are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines execute in, and draw their resources from, resource pools. You can create multiple resource pools as direct children of a standalone host or cluster and then delegate control over them to other individuals or organizations. vCenter Server provides, through the DRS components, various options in monitoring the status of the resources and adjusting or suggesting adjustments to the virtual machines using the resources. You can monitor resources and set alarms on them.
Templates	A master copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed, and can be customized during deployment to ensure that the new virtual machine has a unique name and network settings.
Virtual machines	A virtualized computer environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same managed host machine concurrently.
vApps	VMware vApp is a format for packaging and managing applications. A vApp can contain multiple virtual machines.

Optional vCenter Server Components

Optional vCenter Server components are packaged and installed with the base product, but might require a separate license.

Optional vCenter Server features include:

vMotion A feature that enables you to move running virtual machines from one ESX/ESXi host to another ESX/ESXi host without service interruption. It requires licensing on both the source and target host. vCenter Server centrally coordinates all vMotion activities.

Storage vMotion A feature that allows you to move the disks and configuration file of a running virtual machine from one datastore to another without service interruption. It requires licensing on the virtual machine's host.

VMware HA A feature that enables a cluster with High Availability. If a host goes down, all virtual machines that were running on the host are promptly restarted on different hosts in the same cluster.

When you enable the cluster for HA, you specify the number of hosts you want to be able to recover. If you specify the number of host failures allowed as **1**, HA maintains enough capacity across the cluster to tolerate the failure of one host. All running virtual machines on that host can be restarted on remaining hosts. By default, you cannot turn on a virtual machine if doing so violates required failover capacity. See the *VMware Availability Guide* for more information.

VMware DRS A feature that helps improve resource allocation and power consumption across all hosts and resource pools. VMware DRS collects resource usage information for all hosts and virtual machines in the cluster and gives recommendations (or migrates virtual machines) in one of two situations:

- Initial placement – When you first power on a virtual machine in the cluster, DRS either places the virtual machine or makes a recommendation.
- Load balancing – DRS attempts to improve resource utilization across the cluster by performing automatic migrations of virtual machines (vMotion) or by providing a recommendation for virtual machine migrations.

VMware DRS includes distributed power management (DPM) capabilities. When DPM is enabled, the system compares cluster-level and host-level capacity to the demands of virtual machines running in the cluster. Based on the results of the comparison, DPM recommends (or implements) actions that can reduce the power consumption of the cluster.

VMware Fault Tolerance VMware Fault Tolerance provides continuous availability for virtual machines by creating and maintaining a Secondary VM that is identical to, and continuously available to replace, the Primary VM in the event of a failover situation.

vCenter Server Plug-Ins

vCenter Server plug-ins extend the capabilities of vCenter Server by providing more features and functionality.

Some plug-ins are installed as part of the base vCenter Server product.

vCenter Storage Monitoring	Allows you to review information on storage usage and to visually map relationships between all storage entities available in vCenter Server.
vCenter Hardware Status	Uses CIM monitoring to display the hardware status of hosts managed by vCenter Server.
vCenter Service Status	Displays the status of vCenter services.

Some plug-ins are packaged separately from the base product and require separate installation. You can update plug-ins and the base product independently of each other. VMware modules include:

VMware Update Manager	Enables administrators to apply updates and patches across ESX/ESXi hosts and all managed virtual machines. This module provides the ability to create user-defined security baselines that represent a set of security standards. Security administrators can compare hosts and virtual machines against these baselines to identify and remediate systems that are not in compliance.
VMware Converter	Enables users to convert physical machines and virtual machines in a variety of formats, to ESX/ESXi virtual machines. You can import converted systems into the vCenter Server inventory.
vShield Zones	vShield Zones is an application-aware firewall built for VMware vCenter Server integration. vShield Zones inspects client-server communications and communications between virtual machines to provide detailed traffic analytics and application-aware firewall partitioning. vShield Zones is a critical security component for protecting virtualized datacenters from network-based attacks and misuse.
VMware vCenter Orchestrator	VMware vCenter Orchestrator is a workflow engine that enables you to create and execute automated workflows within your VMware vSphere environment. vCenter Orchestrator coordinates workflow tasks across multiple VMware products and third-party management and administration solutions through its open plug-in architecture. vCenter Orchestrator provides a library of workflows that are highly extensible. You can use any operation available in the vCenter Server API to customize vCenter Orchestrator workflows.
VMware Data Recovery	VMware Data Recovery is a disk-based backup and recovery solution that provides complete data protection for virtual machines. VMware Data Recovery is fully integrated with VMware vCenter Server to enable centralized and efficient management of backup jobs and includes data de-duplication to minimize disk usage.

vSphere Client Interfaces 2

You have several ways to access vSphere components through vSphere interface options.

vSphere interface options include:

vSphere Client — A required component and the primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

vSphere Client is installed on a Windows machine with network access to your ESX/ESXi or vCenter Server system installation. The interface displays slightly different options depending on which type of server you are connected to. While all vCenter Server activities are performed by a vCenter Server system, you must use the vSphere Client to monitor, manage, and control the server. A single vCenter Server system or ESX/ESXi host can support multiple, simultaneously connected vSphere Clients.

vSphere Web Access — A Web interface through which you can perform basic virtual machine management and configuration and get console access to virtual machines. It is installed with your ESX/ESXi host. Similar to the vSphere Client, vSphere Web Access works directly with a host or through vCenter Server. See the *vSphere Web Access Administrator's Guide* for additional information.

VMware Service Console — A command-line interface for configuring an ESX host. For an ESXi host, use the vSphere Command-Line Interface.

vSphere Command-Line Interface — A command-line interface for configuring an ESXi host. The vSphere Command-Line Interface can also be used to perform Storage vMotion operations on both ESX/ESXi hosts.

See Chapter 16, "Starting and Stopping the vSphere Components," on page 203 for information and instructions about starting and stopping ESX hosts and vCenter Server.

This chapter includes the following topics:

Start the vSphere Client and Log In

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

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

Procedure

1 Log in to your Windows system.

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

- If the managed host is not a domain controller, log in as either ***local_host_name**user*** or *user*, where *user* is a member of the local Administrators group.
- If the managed host is a domain controller, you must log in as ***domain**user***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 > vSphere Client**.

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

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

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

4 Click **Login** to continue.

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

Stop the vSphere Client and Log Out

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

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

Procedure

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

The vSphere Client shuts down. The vSphere Client is logged out of the vCenter Server system. The server continues to run all its normal activities in the background. Any scheduled tasks are saved and performed by vCenter Server.

vSphere Web Access

vSphere Web Access is the Web interface through which you can manage your virtual machines. vSphere Web Access is installed when you install ESX/ESXi.

As with the vSphere Client, you can use vSphere Web Access to either connect directly to an ESX/ESXi host or to a vCenter Server system. The functionality of vSphere Web Access is a subset of vSphere Client functionality.

The vSphere Web Access console provides a remote mouse-keyboard-screen (MKS) for the virtual machines. You can interact with a guest operating system running in a virtual machine and connect remotely to the virtual machine's mouse, keyboard, and screen.

- Log In to vSphere Web Access on page 25

  vSphere Web Access uses a Web interface and an Internet connection to access your ESX host or vCenter Server system.

- Log Out of vSphere Web Access on page 25

  Log out when you are finished with your vSphere Web Access activities.

Log In to vSphere Web Access

vSphere Web Access uses a Web interface and an Internet connection to access your ESX host or vCenter Server system.

vSphere Web Access does not have its own concept of users or permissions. Use the same login credentials you would use to log in to the vSphere Client.

Procedure

1 Launch your Web browser.

2 Enter the URL of your ESX or vCenter Server installation:

`https://host_or_server_name/ui`

3 Type your user name and password, and click **Log In**.

After your user name and password are authorized by vSphere Web Access, the vSphere Web Access home page appears.

Log Out of vSphere Web Access

Log out when you are finished with your vSphere Web Access activities.

Procedure

- Click the Log Out link located at the top right corner of every page.

Remote client devices are disconnected when you log out of vSphere Web Access.

VMware Service Console

The service console is typically used only when you contact a VMware technical support representative. In previous versions of ESX, the service console was one of the interfaces to ESX hosts. Many of the commands are now deprecated.

ESXi does not have a service console. Some service console commands are available for ESXi through the remote command-line interface.

The vSphere SDK is used for scripted manipulation of your vSphere instead. The vSphere Client is the primary interface to all nonscripted activities, including configuring, monitoring, and managing your virtual machines and resources.

Using DHCP for the Service Console

The recommended setup is to use static IP addresses for the service console of an ESX host. You can set up the service console to use DHCP, if your DNS server can map the service console's host name to the dynamically generated IP address.

If your DNS server cannot map the host's name to its DHCP-generated IP address, you must determine the service console's numeric IP address. Another caution against using DHCP is that the numeric IP address might change as DHCP leases run out or when the system is rebooted.

VMware does not recommend using DHCP for the service console unless your DNS server can handle the host name translation.

Connect to the Service Console

If you have direct access to the system where ESX is running, you can log in to the physical console on that system.

Whether you use the service console locally or through a remote connection, you must log in using a valid user name and password.

NOTE Depending on the security settings for your ESX computer, you might be able to connect remotely to the service console using SSH or Telnet. For more information see the *ESX Configuration Guide*.

Procedure

- Press Alt+F2 to get to the login screen and log in.

Using Commands on the Service Console

The service console runs a modified version of Linux. Many of the commands available on Linux or UNIX are also available on the service console.

Detailed usage notes for most service console commands are available as manual or `man` pages.

NOTE ESXi does not have a service console. However, many of the functions provided by the service console are available through the vSphere CLI.

View the man Page for a Service Console Command

`man` pages provide information about commands and their usage, options, and syntax.

Procedure

- At the service console command line, type the `man` command followed by the name of the command for which you want to see information.

  For example: `man` *command*

Using the vSphere Client 3

The vSphere Client is the principal interface for administering vCenter Server and ESX/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 ESX/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:

Getting Started Tabs

In the case where 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 28

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

- Restore Getting Started Tabs on page 28

  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**.

Status Bar, Recent Tasks, and Triggered Alarms

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

The status bar appears at the bottom of the window. It contains icons to view triggered alarms or recent tasks. The **Tasks** button displays any currently running or recently completed active tasks. Included is a progress bar indicating the percentage complete of each task. The recent tasks and the triggered alarm panels display across the bottom of the vSphere Client window.

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.

View Virtual Machine Console

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

Procedure

1 Select a powered-on virtual machine.

2 In the Information panel, click the **Console** tab.

3 (Optional) Click the pop-out icon in the navigation bar to show the virtual machine console in a separate window.

4 (Optional) Press Ctrl+Alt+Enter to enter or exit full screen mode.

Searching the vSphere Inventory

The vSphere Client allows you to search your 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**
- **Folders**
- **Hosts**
- **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 search string. The virtual machines reside on hosts whose names match a second search string.

Procedure

1 Select **View > Inventory > Search** to display the advanced search page.

2 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**
- **Folders**
- **Hosts**
- **Datastores**
- **Networks**
- **Inventory**, which finds matches to the search criteria in any of the available managed object types.

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

4 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 Step 4b through Step 4c.

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

5 Click **Search**.

The search results appear below the search specification.

Using Lists

Many vSphere Client inventory tabs display lists of information.

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

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

Filter a List View

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

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

Procedure

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

2 Select the attributes on which to filter.

3 Enter search criteria into the filter field.

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

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

Export a List

You can export a list to a file.

Procedure

1 Select the list to export.

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

3 Type a filename and select a file type.

4 Click **Save**.

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

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 ESX/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. Use annotations 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.

4 To edit the value of an attribute that is already 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** 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** 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 Select **Enable** to enable a plug-in, or deselect **Enable** 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 Plug-Ins

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

vCenter Server plug-ins running on the tomcat server have `extension.xml` files which contain the URL where the corresponding Web application can be accessesed (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 vSphere Clients that will use them must be located on systems under the same domain. If they are not, or 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. Re-register the plug-in after editing its `extension.xml` file.

Save vSphere Client Data

The vSphere Client user interface is similar to a browser. Most user actions are persistent in 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 vCenter Server data. Open the data in an appropriate application and print from that application.

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 ESX/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**.

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.

Setting Up vCenter Server

Using vCenter Server in Linked Mode 4

You can join multiple vCenter Server systems using vCenter Linked Mode to allow them to share information. When a server is connected to other vCenter Server systems using Linked Mode, you can connect to that vCenter Server system and view and manage the inventories of the linked vCenter Server systems.

Linked Mode uses Microsoft Active Directory Application Mode (ADAM) to store and synchronize data across multiple vCenter Server systems. ADAM is installed as part of vCenter Server installation. Each ADAM instance stores data from the vCenter Server systems in the group, including information about roles and licenses. This information is replicated across all of the ADAM instances in the connected group to keep them in sync.

When vCenter Server systems are connected in Linked Mode, you can perform the following actions:

- Log in simultaneously to vCenter Server systems for which you have valid credentials.
- Search the inventories of the vCenter Server systems in the group.
- View the inventories of the vCenter Server systems in the group in a single inventory view.

You cannot migrate hosts or virtual machines between vCenter Server systems connected in Linked Mode.

For more information on troubleshooting Linked Mode groups, see *ESX and vCenter Server Installation Guide*.

This chapter includes the following topics:

Linked Mode Prerequisites

Prepare the system for joining a Linked Mode group.

All the requirements for standalone vCenter Server systems apply to Linked Mode systems. For more information, see *ESX and vCenter Server Installation Guide*.

The following requirements apply to each vCenter Server system that is a member of a Linked Mode group:

- DNS must be operational for Linked Mode replication to work.
- The vCenter Server instances in a Linked Mode group can be in different domains if the domains have a two-way trust relationship. Each domain must trust the other domains on which vCenter Server instances are installed.
- When adding a vCenter Server instance to a Linked Mode group, the installer must be run by a domain user who is an administrator on both the machine where vCenter Server is installed and the target machine of the Linked Mode group.
- All vCenter Server instances must have network time synchronization. The vCenter Server installer validates that the machine clocks are not more than 5 minutes apart.

Linked Mode Considerations

There are several considerations to take into account before you configure a Linked Mode group.

- Each vCenter Server user sees the vCenter Server instances on which they have valid permissions.
- When first setting up your vCenter Server Linked Mode group, you must install the first vCenter Server as a standalone instance because you do not yet have a remote vCenter Server machine to join. Subsequent vCenter Server instances can join the first vCenter Server or other vCenter Server instances that have joined the Linked Mode group.
- If you are joining a vCenter Server to a standalone instance that is not part of a domain, you must add the standalone instance to a domain and add a domain user as an administrator.
- The vCenter Server instances in a Linked Mode group do not need to have the same domain user login. The instances can run under different domain accounts. By default, they run as the LocalSystem account of the machine on which they are running, which means they are different accounts.
- During vCenter Server installation, if you enter an IP address for the remote instance of vCenter Server, the installer converts it into a fully qualified domain name.
- You cannot join a Linked Mode group during the upgrade procedure when you are upgrading from VirtualCenter 25 to vCenter Server 4.1. You can join after the upgrade to vCenter Server is complete. See the *vSphere Upgrade Guide*.

Join a Linked Mode Group After Installation

If you have a system that is already running vCenter Server 4.0 or higher, you can join the machine to a Linked Mode group.

Prerequisites

See "Linked Mode Prerequisites," on page 39 and "Linked Mode Considerations," on page 40.

Procedure

1. Select **Start > All Programs > VMware > vCenter Server Linked Mode Configuration**.
2. Click **Next**.
3. Select **Modify linked mode configuration** and click **Next**.
4. Click **Join this vCenter Server instance to an existing linked mode group or another instance** and click **Next**.
5. Enter the server name and LDAP port number of a remote vCenter Server instance that is a member of the group and click **Next**.

   If you enter an IP address for the remote server, the installer converts it into a fully qualified domain name.

6 If the vCenter Server installer detects a role conflict, select how to resolve the conflict.

Option	Description
Yes, let VMware vCenter Server resolve the conflicts for me	Click **Next**. The role on the joining system is renamed to *vcenter_name role_name,* where *vcenter_name* is the name of the vCenter Server system that is joining the Linked Mode group, and *role_name* is the name of the original role.
No, I'll resolve the conflicts myself	To resolve the conflicts manually: a Using the vSphere Client, log in to one of the vCenter Server systems using an account with **Administrator** privileges. b Rename the conflicting role. c Close the vSphere Client session and return to the vCenter Server installer. d Click **Back** and click **Next**. The installation continues without conflicts.

A conflict results if the joining system and the Linked Mode group each contain a role with the same name but with different privileges.

7 Click **Finish**.

vCenter Server restarts. Depending on the size of your inventory, the change to Linked Mode might take from a few seconds to a few minutes to complete.

The vCenter Server instance is now part of a Linked Mode group. After you form a Linked Mode group, you can log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Servers in the group. It might take several seconds for the global data (such as user roles) that are changed on one machine to be visible on the other machines. The delay is usually 15 seconds or less. It might take a few minutes for a new vCenter Server instance to be recognized and published by the existing instances, because group members do not read the global data very often.

Reconciling Roles When Connecting vCenter Server to a Linked Mode Group

When you join a vCenter Server system to a linked mode group, the roles defined on each vCenter Server system in the group are replicated to the other systems in the group.

If the roles defined on each vCenter Server system are different, the roles lists of the systems are combined into a single common list. For example, if vCenter Server 1 has a role named Role A and vCenter Server 2 has a role named Role B, then both servers will have both Role A and Role B after they are joined in a linked mode group.

If two vCenter Server systems have roles with the same name, the roles are combined into a single role if they contain the same privileges on each vCenter Server system. If two vCenter Server systems have roles with the same name that contain different privileges, this conflict must be resolved by renaming at least one of the roles. You can choose to resolve the conflicting roles either automatically or manually.

If you choose to reconcile the roles automatically, the role on the joining system is renamed to *vcenter_name role_name* where *vcenter_name* is the name of the vCenter Server system that is joining the Linked Mode group and *role_name* is the name of the original role.

If you choose to reconcile the roles manually, connect to one of the vCenter Server systems with the vSphere Client and rename one instance of the role before proceeding to join the vCenter Server system to the Linked Mode group.

If you remove a vCenter Server system from a linked mode group, the vCenter Server system retains all the roles it had as part of the group.

Isolate a vCenter Server Instance from a Linked Mode Group

You can isolate a vCenter Server instance from a Linked Mode group.

Procedure

1 Select **Start > All Programs > VMware > vCenter Server Linked Mode Configuration**.

2 Click **Modify linked mode configuration** and click **Next**.

3 Click **Isolate this vCenter Server instance from linked mode group** and click **Next**.

4 Click **Continue** and click **Finish**.

vCenter Server restarts. Depending on the size of your inventory, the change to Linked Mode configuration might take from a few seconds to a few minutes to complete.

The vCenter Server instance is no longer part of the Linked Mode group.

Change the Domain of a vCenter Server System in a Linked Mode Group

To change the domain of a vCenter Server system in a Linked Mode group, isolate the vCenter Server system from the Linked Mode group first.

vCenter Server systems in a Linked Mode group can be in different domains if the domains have a trust relationship.

Procedure

1 Isolate the vCenter Server system from the Linked Mode group.

2 Change the domain of the vCenter Server system.

Refer to the documentation for the operating system on which vCenter Server is installed for more information on changing the domain.

3 Rejoin the vCenter Server system to the Linked Mode group.

Configure the URLs on a Linked Mode vCenter Server System

If you connect a vCenter Server system to a Linked Mode group and the vCenter Server system has a machine name that does not match the domain name, several connectivity problems arise. This procedure describes how to correct this situation.

If you do not update the URLs, remote instances of vCenter Server cannot reach the vCenter Server system, because the default vCenter Server URL entries are no longer accurate. The vCenter Server installer configures default URL entries as follows:

- For the Virtualcenter.VimApiUrl key, the default value is `http(s)://`*`Fully qualified domain name (FQDN) of vCenter Server machine`*`/sdk`.
- For the Virtualcenter.VimWebServicesUrl key, the default value is `https://`*`FQDN of vCenter Server machine`*`:`*`installed-webservices-port`*`/vws`.

Procedure

1 Isolate the vCenter Server system from the Linked Mode group.

See "Isolate a vCenter Server Instance from a Linked Mode Group," on page 42.

2 Change the domain name or the machine name to make them match.

3 From the vSphere Client, connect directly to the vCenter Server instance on which you have changed the domain or machine name.

4 Select **Administration > vCenter Server Settings** and click **Advanced Settings**.

5 For the Virtualcenter.VimApiUrl key, change the value to point to the location where the vSphere Client and SDK clients can access the vCenter Server system.

For example: `http(s)://machine-name/IP address:vc-port/sdk`.

6 For the Virtualcenter.VimWebServicesUrl key, change the value to point to the location where vCenter Server Webservices is installed.

For example: `https://machine-name/ip:webservices-port/vws`.

7 For the Virtualcenter.Instancename key, change the value so that the modified name appears in the vCenter Server inventory view.

8 Rejoin the vCenter Server system to the Linked Mode group.

See "Join a Linked Mode Group After Installation," on page 40.

Linked Mode Troubleshooting

If you are having trouble with your Linked Mode group, consider the following points.

- When you have multiple vCenter Server instances, each instance must have a working relationship with the domain controller and not conflict with another machine that is in the domain. Conflicts can occur, for example, when you clone a vCenter Server instance that is running in a virtual machine and you do not use sysprep or a similar utility to ensure that the cloned vCenter Server instance has a globally unique identifier (GUID).
- If the domain controller is unreachable, vCenter Server might be unable to start. You might be unable to make changes to the Linked Mode configuration of the affected vCenter Server system.

  If this occurs, resolve the problem with the domain controller and restart vCenter Server. If resolving the problem with the domain controller is not possible, you can restart vCenter Server by removing the vCenter Server system from the domain and isolating the system from its current Linked Mode group.
- The DNS name of the machine must match with the actual machine name. Symptoms of machine names not matching the DNS name are data replication issues, ticket errors when trying to search, and missing search results from remote instances.
- There is correct order of operations for joining a Linked Mode group.

  a Verify that the vCenter Server domain name matches the machine name. If they do not match, change one or both to make them match.

  b Update the URLs to make them compatible with the new domain name and machine name.

  c Join the vCenter Server system to a Linked Mode group.

  If you do not update the URLs, remote instances of vCenter Server cannot reach the vCenter Server system, because the default vCenter Server URL entries are no longer accurate. See "Configure the URLs on a Linked Mode vCenter Server System," on page 42.

  If a vCenter Server instance is no longer reachable by remote instances of vCenter Server, the following symptom might occur:

  - Clients logging in to other vCenter Server systems in the group cannot view the information that belongs to the vCenter Server system on which you changed the domain name because the users cannot log in to the system.
  - Any users that are currently logged in to the vCenter Server system might be disconnected.
  - Search queries do not return results from the vCenter Server system.

To resolve this issue, make sure that the Virtualcenter.VimApiUrl key points to the location where the vSphere Client and SDK clients can access the vCenter Server system, and the Virtualcenter.VimWebServicesUrl key points to the location where vCenter Server Webservices is installed. For the Virtualcenter.Instancename key, change the value so that the modified name appears in the vCenter Server inventory view.

- If you cannot join a vCenter Server instance, you can resolve the problem with the following actions:
  - Ensure that the machine is grouped into the correct organizational unit in the corresponding domain controller.
  - When you install vCenter Server, ensure that the logged in user account has administrator privileges on the machine.
  - To resolve trust problems between a machine and the domain controller, remove the machine from the domain and then add it to the domain again.
  - To ensure that the Windows policy cache is updated, run the `gpupdate /force` command from the Windows command line. This command performs a group policy update.
- If the local host cannot reach the remote host during a join operation, verify the following:
  - Remote vCenter Server IP address or fully qualified domain name is correct.
  - LDAP port on the remote vCenter Server is correct.
  - VMwareVCMSDS service is running.
- Make sure your Windows and network-based firewalls are configured to allow Linked Mode.

Configure a Windows Firewall to Allow a Specified Program Access

vCenter Server 4.1 uses Microsoft ADAM/AD LDS to enable Linked Mode, which uses the Windows RPC port mapper to open RPC ports for replication. When you install vCenter Server in Linked Mode, the firewall configuration on the local machine must be modified.

Incorrect configuration of firewalls can cause licenses and roles to become inconsistent between instances.

Prerequisites

- The Windows version must be an earlier than Windows Server 2008. For Windows Server 2008, Windows automatically configures the firewall to permit access.
- There must be no network-based firewalls between vCenter Server Linked Mode instances. For environments with network-based firewalls, see "Configure Firewall Access by Opening Selected Ports," on page 45.

Procedure

1. Select **Start > Run**.
2. Type **`firewall.cpl`** and click **OK**.
3. Make sure that the firewall is set to allow exceptions.
4. Click the **Exceptions** tab.
5. Click **Add Program**.
6. Add an exception for `C:\Windows\ADAM\dsamain.exe` and click **OK**.
7. Click **OK**.

Configure Firewall Access by Opening Selected Ports

vCenter Server 4.1 uses Microsoft ADAM/AD LDS to enable Linked Mode, which uses the Windows RPC port mapper to open RPC ports for replication. When you install vCenter Server in Linked Mode, the firewall configuration on any network-based firewalls must be modified.

Incorrect configuration of firewalls can cause licenses and roles to become inconsistent between instances.

Procedure

- Configure Windows RPC ports to generically allow selective ports for machine-to-machine RPC communication.

  Choose one of the following methods.

  - Change the registry settings. See http://support.microsoft.com/kb/154596/en-us.
  - Use Microsoft's `RPCCfg.exe` tool. See http://support.microsoft.com/kb/908472/en-us.

Monitor vCenter Server Services

When you are logged in to a vCenter Server system that is part of a connected group, you can monitor the health of services running on each server in the group.

Procedure

- From the vSphere Client Home page, click **vCenter Service Status**.

  You can view the following information in the status window:

  - A list of vCenter Server systems and their services, and vCenter Server plug-ins.
  - Status of all listed items.
  - Date and time when the last change in status occurred.
  - Messages associated with the change in status.

Configuring Hosts and vCenter Server 5

Configuring ESX hosts, vCenter Server systems, and the vSphere Client involves several tasks.

This chapter includes the following topics:

Host Configuration

Before you create virtual machines on your hosts, you must configure the hosts to ensure that they have correct licensing, network and storage access, and security settings. Each type of host has a manual that provides information on the configuration for that host.

- For information on configuring an ESX host, see the *ESX Configuration Guide*.
- For information on configuring an ESXi host, see the *ESXi Configuration Guide*.

Configuring vCenter Server

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

- Configure License Settings for vCenter Server on page 48

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

- Configuring Statistics Settings on page 49

  To set up how statistical data is recorded, you configure statistics intervals.

- Configure Runtime Settings on page 51

  You can change the port number the server is using for communications. You can also 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.

- Configure Active Directory Settings on page 51

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

- Configure Mail Sender Settings on page 52

  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.

- Configure SNMP Settings on page 53

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

- Configure Ports Settings on page 53

  You can configure the ports used by the Web Service to communicate with other applications.

- Configure Timeout Settings on page 54

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

- Configure Logging Options on page 54

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

- Configure the Maximum Number of Database Connections on page 55

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

- Configure Database Retention Policy on page 55

  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.

- Configure SSL Settings on page 56

  You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you select this option, vCenter Server, the vSphere Client, and Web Access clients check for valid SSL certificates before connecting to a host for such operations as adding a host or making a remote console connection to a virtual machine.

- Configure Advanced Settings on page 56

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

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 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 ESX 4.0/ESXi 4.0 keys, select **Home > Administration > Licensing**.

4 (Optional) Enter the fully qualified domain name or the IP address of a license server and, optionally, a port.

A license server is required if this vCenter Server system manages ESX 3.x/ESXi 3.5 hosts or if you have additional vCenter modules that require a license server.

If you do not specify a port, the default port, 27000, is used.

For example, with the default license server port 27000 on a license server called license, your entry might look like this:

```
27000@license.example.com
```

If you do not use the fully qualified domain name or the IP address of the license server, legacy hosts might not be able to resolve the license server host name.

5 (Optional) Select **Reconfigure ESX 3 hosts using license servers to use this server** if you want each ESX 3.x/ESXi 3.5 host that you add to the vCenter Server inventory to use the same license server as this vCenter Server system.

The settings on the host are altered by vCenter Server only when the host is added or when the license server used by vCenter Server is changed. If you leave this option unselected, you can either configure another license server for the ESX 3.x/ESXi 3.5 hosts or configure the hosts to use host-based license files.

Configuring Statistics Settings

To set up how statistical data is recorded, you configure statistics intervals.

- Configure Statistics Intervals on page 49

  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.

- Enable or Disable a Statistics Interval on page 50

  Enabling a statistics interval increases the number of statistics stored in the vCenter Server database. Disabling a statistics interval disables all subsequent intervals and decreases the number of statistics stored in the vCenter Server database.

- Estimate the Effect of Statistics Collection on the Database on page 50

  The impact of the statistics collection on your vCenter database is based on the current vCenter and inventory size.

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 > vCenter Server Settings** to open the **vCenter Server Settings dialog box**.

2 If your environment uses multiple vCenter Servers, in **Current vCenter Server**, select the server.

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

4 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.

5 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.

6 (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.

7 Click **OK**.

Enable or Disable a Statistics Interval

Enabling a statistics interval increases the number of statistics stored in the vCenter Server database. Disabling a statistics interval disables all subsequent intervals and decreases the number of statistics stored in the vCenter Server database.

Required privilege: **Global.Settings**

Prerequisites

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

Procedure

1 Select or deselect the statistics interval check box.

2 Click **OK**.

Estimate the Effect of Statistics Collection on the Database

The impact of the statistics collection on your vCenter database is based on the current vCenter and inventory size.

Required privilege: **Global.Settings**

Prerequisites

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

Procedure

1 If necessary, configure the statistics intervals.

2 In the database calculator pane, specify the number of hosts and virtual machines in your datacenter.

   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.

3 Click **OK**.

Configure Runtime Settings

You can change the port number the server is using for communications. You can also 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 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 pane, select **Active Directory**.

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

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

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

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

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

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

9 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 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 pane, select **Mail**.

4 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

5 Enter the sender account information.

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

For example, mail_server@datacenter.com.

6 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 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 settings list, select **SNMP**.

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

5 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.

6 In **Community**, enter the community identifier.

7 Click **OK**.

Configure Ports Settings

You can configure the ports used by the Web Service to communicate with other applications.

The Web Service is installed as part of the VMware vCenter Server installation. The Web Service is a required component for third-party applications that use the VMware SDK application programming interface (API). For information about Web Service installation, see the *Installation Guide*.

Required privilege: **Global.Settings**

Prerequisites

To configure Ports 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 settings list, select **Ports**.

4 Enter values for the http and https ports.

5 Click **OK**.

What to do next

Restart the vCenter Server system in order for the changes to take effect.

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 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 settings list, select **Timeout Settings**.

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

Do not set the value to zero (0).

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

Do not set the value to zero (0).

6 Click **OK**.

7 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 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 settings list, select **Logging Options**.

4 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
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

5 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 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 settings list, select **Database**.

4 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.

5 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 enter 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 enter 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.

Configure SSL Settings

You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you select this option, vCenter Server, the vSphere Client, and Web Access clients check for valid SSL certificates before connecting to a host for such operations as adding a host or making a remote console connection to a virtual machine.

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 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 **Current vCenter Server**, select the appropriate server.

4 In the settings list, select **SSL Settings**.

5 Select **vCenter requires verified host certificates**.

If there are hosts that require manual validation, these hosts appear in the host list at the bottom of the dialog box.

6 Determine the host thumbprint for each host that requires validation.

- For ESX hosts, log into the service console and type `openssl x509 –in /etc/vmware/ssl/rui.crt –fingerprint –sha1 –noout`.
- For ESXi hosts, log into the direct console and select **View Support Information** on the System Customization menu. The thumbprint is displayed in the column on the right.

7 Compare the thumbprint you obtained from the host with the thumbprint listed in the vCenter Server Settings dialog box.

8 If the thumbprints match, select the check box for the host.

Hosts that are not selected will be disconnected after you click **OK**.

9 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 VI 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 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 settings list, select **Advanced Settings**.

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

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

6 Click **Add**.

7 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 ESX, vCenter Server, and the vSphere Client

By default, the vSphere Client uses ports 80 and 443 to communicate with vCenter Server and ESX/ESXi hosts. You can change these ports if necessary.

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.

Setting Up Your Virtual Infrastructure

Organizing Your Inventory

6

Plan how you will set up your virtual infrastructure. A large vSphere implementation might contain several virtual datacenters with a complex arrangement of hosts, clusters, resource pools, and networks. It might involve multiple vSphere Servers operating in Linked Mode. Smaller implementations might require a single virtual datacenter with a much less complex topology. Regardless of the scale of your virtual infrastructure, 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 vNetwork Distributed Switches?
- 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.

Populating and organizing your inventory involves the following activities:

This chapter includes the following topics:

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 *ESX Configuration Guide* and the *ESXi Configuration Guide*.

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.

This option is available for ESXi hosts only. 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 VMware High Availability (HA) and VMware 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 Select **Home > Inventory > Hosts and Clusters**.

2 Select a datacenter or folder within a datacenter.

3 Select **File > New > Cluster**.

4 Enter a name for the cluster and select features that you want to use with it, and click **Next**.

5 Choose cluster features.

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

6 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.

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

8 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 vSphere Client is logged in to a vCenter Server.
- 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 vNetwork Standard Switches (vSwitch) 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 vNetwork Distributed Switches, uplink 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 Click **Networking**.

4 Click **Virtual Switch**.

5 Click **Add Networking**.

6 Select a connection type.

7 Select an existing virtual switch or create one.

8 Enter a display label for the port group on the switch.

9 Select a VLAN ID.

10 Review your settings and click **Finish**.

If you chose to use an existing vSwitch, a new port group is added to it. If you chose to create a vSwitch, 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 vNetwork Standard Switches (vSwitch) 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 vNetwork Distributed Switches, uplink 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 **Home > Inventory > Networking** view, and select a datacenter.

2 Click **New vNetwork Distributed Switch** in the toolbar.

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

4 Enter a display name for the switch.

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

6 Add hosts and their physical network adapters to the switch and click **Next**.

7 Choose whether you want vSphere to automatically create a port group and click **Finish**.

A vNetwork Distributed Switch, with its associated dvUplink 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 vNetwork Distributed Switch Settings

Use the vNetwork Distributed Switch Settings dialog box to configure general vNetwork Distributed Switch settings such as the vNetwork Distributed Switch name and the number of uplink ports on the vNetwork Distributed Switch.

Procedure

1 In the vSphere Client, select the Networking inventory view and select the vNetwork Distributed Switch.

2 From the **Inventory** menu, select **vNetwork Distributed Switch > Edit Settings**.

3 Select **General** to edit the vNetwork Distributed Switch properties.

Option	Description
Name	Enter the name for the vNetwork Distributed Switch.
Number of Uplink Ports	Select the number of uplink ports for the vNetwork Distributed Switch. To edit uplink port names, click **Edit uplink port names**, enter new names for the uplinks, and click **OK**.
Notes	Enter any notes for the vNetwork Distributed Switch.

4 Click **OK**.

Edit Advanced vNetwork Distributed Switch Settings

Use the vNetwork Distributed Switch Settings dialog box to configure advanced vNetwork Distributed Switch settings such as Cisco Discovery Protocol and the maximum MTU for the vNetwork Distributed Switch.

Procedure

1 In the vSphere Client, select the Networking inventory view and select the vNetwork Distributed Switch.

2 From the **Inventory** menu, select **vNetwork Distributed Switch > Edit Settings**.

3 Select **Advanced** to edit the following vNetwork Distributed Switch settings.

Option	Description
Maximum MTU	The maximum MTU size for the vNetwork Distributed Switch.
Enable Cisco Discovery Protocol	Check this box to enable Cisco Discovery Protocol, and set the **Operation** to **Listen**, **Advertise**, or **Both**. For information about Cisco Discovery Protocol, see the *ESX Configuration Guide* and the *ESXi Configuration Guide*.
Admin Contact Info	Enter the **Name** and **Other Details** for the vNetwork Distributed Switch administrator.

4 Click**OK**.

Add Hosts to a vNetwork Distributed Switch

You can add hosts and physical adapters to a vNetwork Distributed Switch at the vDS level after the vDS is created.

Procedure

1 In the vSphere Client, select the Networking inventory view and select the vNetwork Distributed Switch.

2 Select **Inventory > vNetwork Distributed Switch > 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 free and in use.

NOTE Moving a physical adapter to a vDS without moving any associated virtual adapters can cause those virtual adapters to lose network connectivity.

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

6 Click **Next**.

7 (Optional) Migrate virtual machine networking to the vDS.

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 Review the settings for the vDS, and click **Finish**.

If you need to make any changes, click **Back** to the appropriate screen.

Add a dvPort Group

Use the Create dvPort Group wizard to add a dvPort group to a vNetwork Distributed Switch.

Procedure

1 In the vSphere Client, select the Networking inventory view and select the vNetwork Distributed Switch.

2 Select **Inventory > vNetwork Distributed Switch > New Port Group**.

The Create dvPort Group wizard appears.

3 Enter a **Name** and the **Number of Ports** for your new dvPort 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 have not created any private VLANs, this menu is empty.

5 Click **Next**.

6 Click **Finish**.

Edit General dvPort Group Settings

Use the dvPort Group Properties dialog box to configure general dvPort group properties such as the dvPort group name and port group type.

Procedure

1 In the vSphere Client, display the Networking inventory view and select the dvPort group.

2 From the **Inventory** menu, select **Network** > **Edit Settings**.

3 Select **General** to edit the following dvPort group properties.

Option	Action
Name	Enter the name for the dvPort group.
Description	Enter a brief description of the dvPort group.
Number of Ports	Enter the number of ports on the dvPort group.
Port binding	Choose when ports are assigned to virtual machines connected to this dvPort group. ■ Select **Static binding** to assign a port to a virtual machine when the virtual machine is connected to the dvPort group. ■ 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 dvPort group. ■ Select **Ephemeral** for no port binding. You can choose ephemeral binding only when connected directly to your ESX/ESXi host.

4 Click **OK**.

Edit Advanced dvPort Group Settings

Use the dvPort Group Settings dialog box to configure advanced dvPort group properties such as the port name format and override settings.

Procedure

1 In the vSphere Client, display the Networking inventory view and select the dvPort group.

2 From the **Inventory** menu, select **Network** > **Edit Settings**.

3 Select **Advanced** to edit the dvPort group properties.

Option	Description
Allow override of port policies	Select this option to allow dvPort 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 dvPort is disconnected from a virtual machine, the configuration of the dvPort is reset to the dvPort group setting. Any per-port overrides are discarded.

4 Click **OK**.

Managing ESX/ESXi and vCenter Server Licenses

7

License reporting and management are centralized.

All product licenses are encapsulated in 25-character license keys that you can manage and monitor from vCenter Server.

Licensing is applicable to ESX/ESXi hosts, vCenter Server, and solutions. However, solutions licensing management is specific to the solution. For solutions, licensing can be based on processors, asset instances, virtual machines, and so on. Therefore, the licensing for a solution such as VMware vCenter Site Recovery Manager might differ entirely from the licensing of another solution. For information about licensing a specific solution, see the documentation for that solution.

Each host requires a license, and each vCenter Server instance requires a license. You cannot assign multiple license keys to a host or to a vCenter Server system. You can license multiple hosts with one license key if the key has enough capacity for more than one host. Likewise, you can license multiple vCenter Server instances with one license key if the key has a capacity greater than one and you can license multiple solutions with one license key if the key has a capacity greater than one. When you apply a minor upgrade or patch the ESX/ESXi or vCenter Server software, you do not need to replace the existing license key with a new one.

In terms of licensing hosts, if you upgrade all your hosts, you no longer need a license server or host-based license files.

If you upgrade the edition of the license (for example, from standard to enterprise), you must replace the existing license key in the inventory with a new upgraded license key.

This chapter includes the following topics:

About License Key Capacity

License keys have a certain amount of capacity. For hosts, capacity is based on the number of processors in the host. For vCenter Server, capacity is based on the number of instances of vCenter Server. However, the licensing of solutions can be based on processors, asset instances, virtual machines, etc.

The examples that follow might not apply to all solutions.

Though licensing is applicable to solutions as well as ESX/ESXi hosts and vCenter Server, solutions licensing management is too variable and, therefore, specific to each solution to be discussed in general terms. For information about licensing a specific solution, see the documentation for that solution.

Licensing for Each Processor

For most vSphere products, when you purchase vSphere licenses, you must consider the total number of processors, not hosts, that will run the products. You can assign and reassign the processor capacity to any combination of hosts. For example, suppose you purchase a 10-processor vSphere license key. You can assign the 10-processor license key to any of the following combinations of hosts:

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

Special considerations include:

- Dual-core and quad-core processors, such as Intel processors that combine two or four independent CPUs on a single chip, count as one processor.
- You cannot partially license a multiprocessor host. For example, a 4-CPU host requires 4-processors of vSphere license key capacity.

IMPORTANT From the ESX/ESXi license perspective, a CPU is a processor with a physical processor in it. When you purchase a license, you select the edition, the number of CPUs, and the maximum number of cores per CPU. For example, if you purchase an enterprise license with 100 CPUs, you must also choose the maximum number of cores per CPU. For example, you might select a maximum of 2 cores per CPU, 6 cores per CPU, or 12 cores per CPU. The choice depends on the type of hardware on which you are installing ESX/ESXi.

Licensing for Each Asset Instance

Products for which you purchase a license for each instance require a single unit of license key capacity, regardless of the number of processors in the machine. The vCenter Server is an example of a product that requires this type of license. If you purchase a vCenter Server license key with a capacity greater than one, you assign one unit of the capacity to each instance of vCenter Server.

About vSphere and vCenter Server License Keys

The terms vSphere and vCenter Server are used for licenses. Solution licenses are listed under the product name for the solution.

vSphere Licenses	For ESX/ESXi.
vCenter Server Licenses	For vCenter Server (formerly, VirtualCenter).
Solution Licenses	For solutions.

About Using a License Server to Manage ESX 3.x/ESXi 3.5 Hosts

vCenter Server 4.1 does not require a license server to manage ESX 4.1/ESXi 4.1 or ESX/ESXi 4.0 hosts. However, vCenter Server 4.1 requires a license server to manage ESX 3.x/ESXi 3.5 hosts.

If you do not have a license server installed and you need one, download the VMware License Server from the VMware Web site.

The License Server installation requires no downtime. No virtual machines, servers, hosts, or clients need to be powered off for the installation of the license server.

Configure vCenter Server to Use a License Server

To manage ESX 3.x/ESXi 3.5 hosts, you must configure vCenter Server to use a license server.

Prerequisites

You must have a license server installed. You can download the VMware License Server from the VMware Web site.

Procedure

1 In vCenter Server, select **Administration > vCenter Server Settings**.

2 In the License Server text box, enter the port number and license server machine name, as in port@host.

For example: 27000@license-3.companyname.com

3 If you want the hosts and vCenter Server to use the same license server, select the **Reconfigure ESX 3 hosts using license servers to use this server** check box.

4 Click **OK**.

About the License Portal

Use the license portal to get upgraded license keys, downgrade license keys, combine the capacity of multiple license keys, divide the capacity of a single license key, view the change history of your license keys, and find lost license keys.

Getting Upgraded License Keys

If you have VMware Infrastructure 3 license keys and you have been provided upgrades to vSphere 4.1 or higher, use the license portal to retrieve the new license keys and deactivate the old licenses. After you retrieve the license keys, enter them into the vCenter Server license inventory.

Downgrading License Keys

If you have license keys for vSphere 4.1 or higher but you need to license VMware Infrastructure 3 or vSphere 4.0 assets, use the license portal to downgrade the license keys. When you do this, the vSphere 4.1 license keys remain valid. When you are ready to upgrade your assets, you can stop using the VMware Infrastructure or vSphere licenses and start using the vSphere 4.1 license keys by entering them into the vCenter Server license inventory and assigning them to your upgraded assets.

Combining the Capacity of License Keys

If your license inventory contains multiple license keys, each with a small amount of capacity, you might want to combine them into one large-capacity license key. This is useful when the total available capacity across license keys is large enough to accommodate an asset, but no single license key is large enough to accommodate the asset.

After you use the license portal to combine license keys, you must add the new license key to the vCenter Server license inventory and remove the old license keys.

Dividing the Capacity of License Keys

If you have a large-capacity license key, you might want to divide the capacity to create multiple smaller-capacity license keys. This is useful for managing license keys in different vCenter Server inventories or assigning different license keys to groups in your organization.

Viewing the Change History of License Keys

The license portal tracks the complete history of license key upgrades, downgrades, combinations, and divisions for your organization.

Finding Lost License Keys

If a license key is misplaced, you can search for it in the license portal using the following criteria:

- Date range
- License key
- Order number
- Transaction type

About License Inventories

The license inventories that are maintained by a vCenter Server system work slightly differently, depending on whether you have Linked Mode groups or standalone systems.

The examples that follow are specific to ESX/ESXi hosts and might not apply to solutions.

Solutions vary greatly. For example, some solutions are not licensed separately from vCenter Server. Furthermore, solutions licensing can be based on processors, asset instances, virtual machines, and so on. Therefore, for license information specific to a solution, see the documentation for that solution.

Example: Uninstallation Scenarios

1 You uninstall vCenter Server without first unlicensing and removing the hosts.

2 The hosts remain licensed.

3 You add the licensed hosts to another vCenter Server instance.

4 The license keys are transferred with the hosts.

Here is a slightly different scenario:

1 You uninstall vCenter Server without first unlicensing the hosts.

2 You reinstall vCenter Server and make it part of a different Linked Mode group.

3 The host license keys from the previous group are not transferred to the new group.

4 You add hosts that were licensed by the previous vCenter Server group to the new group.

5 The host license keys are transferred to the new group.

6 The host license keys now belong to two Linked Mode groups. If the total assignment of the key exceeds the key's capacity, this scenario is not supported and causes your license usage to be out of compliance.

Example: Standalone Scenario

Each vCenter Server instance maintains its own license inventory. If you add an ESX/ESXi host to vCenter Server and add the same host to another vCenter Server instance, the host license key moves from the first inventory to the second inventory.

1 You have two vCenter Server instances that are standalone.

2 You assign a license to a host in one vCenter Server instance.

3 You add the host to another vCenter Server instance and choose to retain the license when you perform the Add Host operation.

4 The host license key belongs to two separate license inventories. If the total assignment of the key exceeds the key's capacity, this scenario is not supported and causes your license usage to be out of compliance.

Example: Linked Mode Scenario

1 You have two vCenter Server instances that belong to the same Linked Mode group.

2 You assign a license to a host in one vCenter Server instance.

3 The two vCenter Server instances share a single license inventory.

4 When you add a license key, the key becomes available to all the vCenter Server systems within the same Linked Mode group. The license keys are shared, and each system in the group has the same inventory view, although this might not always seem so because of replication delays.

Controlling License Permissions

You can control which users are able to view and manage license resources.

The following permission types are supported.

Global.licenses	If you have global permission at the root folder, you can view and modify all licenses in the vCenter Server inventory. This includes other vCenter Server systems in a Linked Mode group.
Read-only	If you have read-only permission on a host, the vCenter Server displays the first and last five characters of the license key assigned to the host, the features present in the license, and the expiration date for the license.

If you have neither of these permissions but you can add a host to vCenter Server, you can add a license to the inventory and assign a license to the host when you perform the add host operation.

View License Information

You can see all the licenses assigned or available in your vSphere inventory using the licensing view.

Procedure

1 From a vSphere Client session that is connected to a vCenter Server system, click **Home > Licensing**.

2 (Optional) Click **Refresh**.

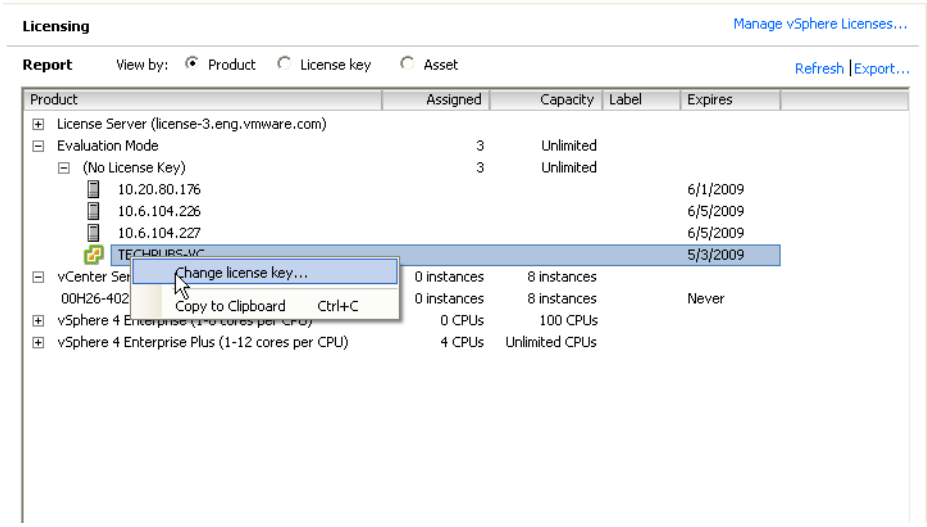
3 On the licensing page, select the view.

- To view the available licenses listed by product, select **Product**.
- To view the available licenses listed by license key, select **License key**.
- To view licenses listed by the asset (host, vCenter Server system, or solution) to which they are assigned, select **Asset**.

From these report views, you can right-click entities to add, assign, and remove license keys and copy license information to your clipboard.

Example: Use the Product View to Add and Assign a License Key

In this example, you select the **Product** view in the Licensing Report window. In the Evaluation Mode list, right-click a vCenter Server instance and select **Change license key**. You can then assign a license key that is in the license inventory or add a new license key and assign it in a single operation.



What to do next

If you have a license with zero assigned capacity, as seen in the Assigned column of the License Report, ask yourself the following questions:

- Did I forget to assign this license key to an asset?
- Did I forget to remove this license key from the inventory?

  Remove the license key in the following cases:

  - The license key has expired.
  - You use the license portal to combine the capacities of multiple small-capacity license keys to create a larger-capacity license key. Then you remove the old license keys and add the new license key to the vCenter Server inventory.
  - You have upgraded your licenses, and you must remove the legacy licenses.

Add a License Key to the License Inventory and Assign It to an Asset

After you purchase an asset, you can add the license key to the inventory and assign it to the asset. Use this procedure to add one license key and assign it to one asset.

Prerequisites

The vSphere Client must be connected to the vCenter Server system.

Procedure

1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.

2 For the report view, select **Asset**.

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

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

5 Enter the license key, enter an optional label for the key, and click **OK**.

6 Click **OK**.

Add Multiple License Keys to the License Inventory

After you purchase assets, you can add the license keys to the license inventory. You can add multiple license keys at the same time.

Prerequisites

The vSphere Client must be connected to the vCenter Server system.

Procedure

1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.

2 Click **Manage vSphere Licenses**.

3 In the Add License Keys text area, enter license keys one per line.

You can paste a list of keys in one operation.

4 (Optional) Type a brief description of the keys.

5 Click **Add License Keys**.

If any of the keys are invalid, an error message lists the invalid keys. You can correct the invalid keys and try adding them again, or delete them.

6 If you are not ready to assign license keys to assets, click **Next** through the remaining wizard screens and click **Finish** to save your changes.

Assign a License Key to Multiple Assets

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

Though licensing is applicable to solutions as well as ESX/ESXi hosts and vCenter Server, solutions licensing management is too variable and, therefore, specific to each solution to be discussed in general terms. For information about licensing a specific solution, see the documentation for that solution.

NOTE After you assign a license to a host, the software might update the license report before the license assignment operation is complete. If the host becomes disconnected immediately after you assign the license, the license report might not accurately reflect the host license state. The report might show the host as licensed, even though the license assignment operation is not yet complete. When the host is reconnected to a vCenter Server system, the license assignment operation continues, and the host becomes licensed as shown in the report.

Procedure

1 From a vSphere Client session that is connected to a vCenter Server system, select **Home > 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 Click **Show Unlicensed assets**, **Show licensed assets**, or **Show all**.

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

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

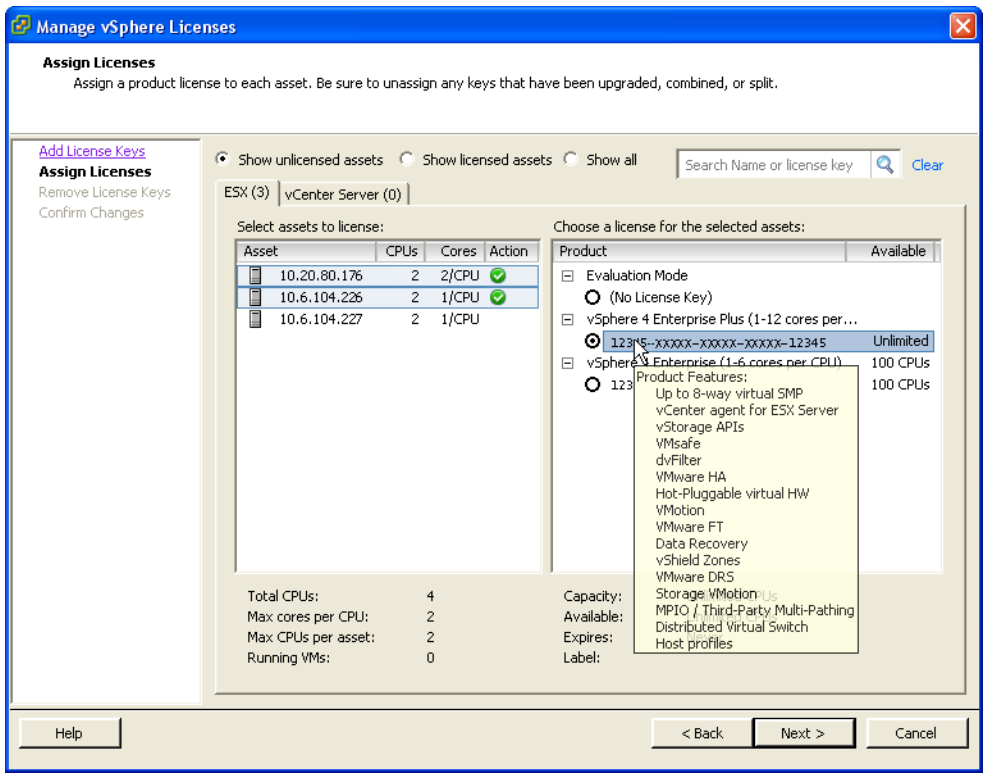
7 In the Product window, select an appropriate license key and click **Next**.

The capacity of the license key must be greater than or equal to the sum of the asset CPUs.

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.

Example: Assign a License Key to Two ESX Hosts

In this example, Shift-click to select two 2-CPU ESX hosts and then assign a vSphere Enterprise license key to the hosts. Before the assignment, the license key has an available capacity of 98 CPUs. After the assignment, the license key has an available capacity of 94 CPUs. The pop-up tool tip lists the product features included in the vSphere Enterprise license edition.



Export Report Data

You can export license data to a file that you can open in a third-party application.

Procedure

1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.

2 Select the view that you want to export.

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

3 From the report screen, 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**.

License a Host Without vCenter Server

If you are directly connected to the host through the vSphere Client, you can license the host.

Procedure

1 From the vSphere Client, click the **Configuration** tab.

2 Under Software, click **Licensed Features**.

3 Click **Edit**.

4 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 enter a license key and an optional label for the license key.

5 Click **OK**.

License a Host When Adding It to the vCenter Server Inventory

When you add a host to the vCenter Server inventory, you can license the host.

Prerequisites

You must have a communication channel through a firewall before adding a host.

Procedure

1 Click **Inventory** in the navigation bar.

2 Expand the inventory as needed and click the appropriate datacenter, folder, or cluster.

3 Right-click the datacenter or cluster and select **Add Host**.

4 When prompted by the Add Host wizard, assign an existing vSphere license key or add a new vSphere license key.

View Which Features Are Licensed on a Host

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

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

Procedure

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

2 Click the **Configuration** tab.

3 Under Software, click **Licensed Features**.

The **Licensed Features** window displays the list of features that you can configure on the host.

Set an ESX/ESXi Host to Evaluation Mode

If you entered a license for ESX or ESXi, you can switch to evaluation mode to explore the full functionality of ESX or ESXi.

Procedure

1 From the vSphere Client connected to a vCenter Server, select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, click **Licensed Features**.

4 Click **Edit** next to**ESX/ESXi License Type**.

5 Click **Product Evaluation**.

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

About the Licensing Reporting Manager

The Licensing Reporting Manager provides a centralized interface for viewing license usage for vCenter Server 4.1 instances, either standalone or in Linked Mode. You access the Licensing Reporting Manager through the vSphere Client.

Using the Licensing Reporting Manager, you can view and generate reports on assigned license keys and their usage for different time periods. The Licensing Reporting Manager provides information about asset assignment, product edition, current usage, average usage, and capacity for each license key used in the inventory. Information does not appear for unused license keys.

The Licensing Accounting Module in vCenter Server takes snapshots of license usage several times a day and stores them in the vCenter Server database. Using the Licensing Reporting Manager, you can see aggregated usage statistics for selected time periods as well as download the collected license usage snapshots for further analysis and processing.

You can download the license data from the Licensing Reporting Manager to CSV format.

You can monitor the Licensing Reporting Manager through the Licensing Accounting Module health monitor on the vCenter Server Status page.

NOTE The Licensing Reporting Manager helps you track current and historical license usage. For license management features such as adding, removing, and assigning license keys, use the Licensing view in the vSphere Client.

About Licensing Reports

You can view and download license usage data with the Licensing Reporting Manager. You can export the licensing report shown in the Licensing Reporting Manager to a CSV file contained in a generated ZIP file. This process allows you to create custom analysis solutions.

Table 7-1 shows the licensing information that the license usage report lists. Usage and averages of usage are calculated for the time period selected. Calculations are based on snapshots that are taken by vCenter Server several times a day.

Table 7-1. Information in the Licensing Report

Licensing Reporting Manager Data		Description
Product		Product to which license keys are assigned. Expand the product to view the license keys for that product.
Average	Usage	Average usage of the license key for the selected time period. Periods when the license key is not assigned (within the selected time period) are excluded when the average usage is calculated. This average is calculated by taking the average of the usage indicated by the set of daily snapshots for the selected period.
	License Capacity	Average purchased license capacity for the selected time period.
	% Usage	Average license usage as a percentage of the average license capacity for the selected time period.
Current	Usage	Current usage of the product or license key.
	License Capacity	Current license capacity of the product or license key.
	% Usage	Current license usage as a percentage of the current license capacity.
Threshold-Current Usage		Allows editing of the threshold value for the product selected. Applies only to products with per-virtual machine licensing. This information is listed only if a single vCenter Server is selected. For CPU- and instance-based licenses (for example, ESX/ESXi and vCenter Server licenses), no data is listed in this column.

The licensing usage information in the licensing report differs from the license usage download. The information in the license report that you can view in the Licensing Reporting Manager is the aggregate usage information for the product or product group over the time period you select.

The download report lists raw data on license usage for the product or product group over the time period you select. All of the snapshots collected for the selected time period are included in the downloaded report with no aggregations applied. The download report can contain host, vCenter Server, or solution asset IDs, but no user-defined names are included. The download report is free of user and company-sensitive information.

Each row of the download report .csv file lists a single license usage snapshot, which includes an asset, its assigned license key, and the usage at the given timestamp. Table 7-2 describes how the license usage information is organized in the download report .csv file.

Table 7-2. Information in the Download Report

Download Report Data	Description
License Key	The assigned license key.
Product Edition	The product edition of the vCenter Server, host, or solution.
Cost Unit	The capacity type of the license key (CPU, instance, virtual machine, and so on)
License Key Expiration Date	If applicable.
Asset ID	The automatically generated ID of the asset used by vCenter Server to identify the asset.
Usage	The usage of the asset from the license key at the time of the timestamp. The unit of this value is indicated in the Cost Unit column.
Capacity	The capacity of the license key. The unit of this value is indicated in the Cost Unit column.

Table 7-2. Information in the Download Report (Continued)

Download Report Data	Description
vCenter Servers	The vCenter Server instances this usage is reported on. This column is useful when the report is generated for multiple vCenter Server instances.
Timestamp	Timestamp of the snapshot.

The last section of raw data in the file contains a signature that is a checksum of the file content. You can ignore this section of the report.

View Licensing Usage Reports with the Licensing Reporting Manager

Use the Licensing Reporting Manager to view licensing usage by vCenter Server and time period.

Prerequisites

Make sure that you have the **Global.Licenses** privilege.

Procedure

1 In the vSphere Client, click **Home > Administration > Licensing Reporting Manager**.

2 (Optional) Select the vCenter Server or the Linked Mode group in the vCenter Servers list for which you want to view licensing information.

By default, the vCenter Server instance you are connected to is selected. vCenter Server instances for versions earlier than vCenter Server 4.1 or instances where the VMware VirtualCenter Management Webservices Windows service is down appear dimmed.

3 (Optional) Select a preconfigured or custom time period for the licensing report using the **Time period** drop-down list.

By default, the YTD period is selected. If you select a custom time period, click **Recalculate** after you select the start and end dates for the report.

The Licensing Reporting Manager lists the license keys by product edition. Expand the product to view the list of license keys assigned to that product.

What to do next

You can download the raw data used to calculate the aggregated information shown and use it to apply further analysis or keep it for your records.

Download a Licensing Report

You can download the licensing report from the Licensing Reporting Manager to CSV format. You can export the licensing information that appears in the Licensing Reporting Manager to a CSV file contained in a generated ZIP file.

NOTE The licensing information listed in the Licensing Reporting Manager is protected in the vCenter Server database by a tamper-detection feature. If the licensing data in the vCenter Server database has been edited, you cannot download the licensing report.

Prerequisites

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

Procedure

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

2 Select the vCenter Server or the Linked Mode group in the vCenter Servers list for which you want to view licensing information.

3 Select the time period for the licensing report using the **Time period** drop-down list.

4 Click **Download report**.

5 (Optional) To view the report, click **Open**.

The default file compression application for the system displays the contents of the .zip file containing the report in CSV format. Double-click the CSV file to view the report. Typically, Microsoft Excel is the default application for CSV files.

6 Click **Save** and browse to the location where you want to save the file.

Set a Threshold for License Usage

You can set a threshold on the current license usage for a product. If the threshold is exceeded, an alarm is triggered on the corresponding vCenter Server instance. License usage thresholds allow administrators to monitor license usage for certain products and trigger notifications if a certain usage is exceeded.

Thresholds apply only to assets with per-virtual machine licensing. Thresholds can be set below or above the purchased license capacity. Thresholds are used for notifications only. Thresholds do not enforce license usage limits.

Prerequisites

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

Procedure

1 (Optional) In the Licensing Reporting Manager, select a vCenter Server instance.

By default, the vCenter Server instance you are connected to is selected. Threshold information can be edited for one vCenter Server instance at a time.

2 Click **Edit** in the threshold column for a product.

3 Enter a number of virtual machines for the threshold.

Click **Clear** to remove the currently set threshold.

4 Click **OK**.

An alarm triggers on the associated vCenter Server and a notification message appears in the Licensing Reporting Manager if the threshold is exceeded. However, no enforcement is made on further use of the product.

NOTE It might take several minutes for the notifications to appear after a threshold is exceeded.

Troubleshooting Licensing

These topics provide guidelines for troubleshooting your license setup for environments with only ESX 4.1/ESXi 4.1 hosts and environments that have a mixture of ESX 4.1/ESXi 4.1 and legacy ESX 3.x/ESXi 3.5 hosts.

If you cannot resolve the problem, contact VMware for support as follows:

- If you have difficulties in configuring licensed features, file a support request at http://www.vmware.com/support.
- To license vCenter Server, you must apply a vCenter Server license key.
- To license ESX/ESXi, you must apply a vSphere license key.

- If you downgrade your license from evaluation mode to a license that does not support the features that you configured while using evaluation mode, the features might stop working without warning.
- If a licensing-related error message appears when you try to configure a feature, check the licensed features on the host and on the vCenter Server system to make sure that the host or vCenter Server system is licensed to use the feature that you are trying to configure.
- If all the hosts in a vCenter Server system inventory become disconnected, this might be because the vCenter Server license is expired or the 60-day evaluation period has expired.
- If you cannot power on the virtual machines that reside on a host, this might be because the host license is expired or the 60-day evaluation period is expired.
- If an ESX/ESXi host is managed by a vCenter Server system, changes made to the host license via direct connection to the host do not persist, because the changes are overwritten by the license key assigned via vCenter Server. See "About Overriding the Host License Configuration," on page 86.
- If vCenter Server is managing ESX 3.x/ESXi 3.5 hosts, vCenter Server must check out vCenter Server Agent licenses from a license server. If vCenter Server is having trouble communicating with your license server, do the following:
  - Check that the license server Microsoft Windows service is running.
  - Check that the license server is listening.
  - Check the license server status.

    If your license server is operating properly, you might have a problem with your license file.

    If your license server is working correctly and your license file is correct, check that you correctly configured centralized or single-host licensing, as appropriate to your environment.

    For detailed troubleshooting and configuration instructions, see the licensing documentation in the *Installation Guide* or the *Setup Guide* for VMware Infrastructure 3.

Applying Licenses

If you cannot apply a license to an asset, the license might not match the currently configured features and resources. When you assign a license to an asset, the license must be compatible with all the configured resources and features.

For example, suppose you add 10 hosts to the vCenter Server inventory during the evaluation period. After the evaluation period expires, you try to assign a Foundation edition license to a vCenter Server system. The assignment operation fails because the Foundation edition allows a vCenter Server system to manage up to three hosts only. To correct this issue, you can upgrade the edition or you can remove seven hosts from the inventory.

As another example, suppose that you configure vMotion and DRS on a cluster of Enterprise edition hosts. Later, you try to assign Standard license keys to the hosts. This operation fails because the Standard edition does not include vMotion and DRS. You must assign Enterprise licenses to the hosts or disable vMotion and DRS. For detailed information about how to disable features, see the VMware Knowledge Base.

Also, make sure you are applying the correct license key, as follows:

- To license vCenter Server assets, you must apply a vCenter Server license key.
- To license ESX/ESXi assets, you must apply a vSphere license key.

About Overriding the Host License Configuration

If the host is managed by vCenter Server, use either the **Home > Licensing** interface or the Add Host operation to configure host licensing.

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

License Expiration

Upon license expiration, the vCenter Server software and the ESX/ESXi software continue to run, but certain operations stop working.

If a vCenter Server license expires, the managed hosts become disconnected from the vCenter Server inventory, and you cannot add hosts to the inventory. The hosts and the virtual machines on the hosts continue to run. By using the vSphere Client to connect directly to the host, you can power on or reset the virtual machines.

After you assign a valid vCenter Server license, you can reconnect all the hosts at once as follows:

1 From the vCenter Server inventory, select the datacenter.

2 Select the **Hosts** tab.

3 Shift-click or Ctrl-click to select the hosts.

4 Right-click and select **Connect**.

If an ESX/ESXi host license expires, the virtual machines that reside on the host continue to run, but you cannot power on the virtual machines or reset them.

Licensing vCenter Server and ESX/ESXi After Evaluation

After the 60-day evaluation period expires, you are no longer able to perform some operations in vCenter Server and ESX/ESXi. If you want to continue to have full use of ESX/ESXi and vCenter Server operations, you must acquire a license.

Without a license, you are able to perform some operations, but you cannot power on or reset your virtual machines. All hosts are disconnected from the vCenter Server system if the evaluation period expires before you assign a license to the vCenter Server system. Any single ESX/ESXi host is disconnected from the vCenter Server system if the ESX/ESXi evaluation period expires before you assign a license to the host.

When you switch your vCenter Server system and ESX from evaluation mode to licensed mode, consider the following:

- If a vCenter Server system is managing VMware Infrastructure 3 hosts (for example, ESX 3.x or ESXi 3.5), the vCenter Server system must have access to a license server. You can download the VMware License Server from the VMware Web site.
- To license vCenter Server, you must apply a vCenter Server license key.
- To license ESX/ESXi, you must apply a vSphere license key.
- When you assign a license to a machine on which a VMware vSphere component is installed, the license must be compatible with all resources and features that you configure during the evaluation period.

  For example, suppose you add 10 hosts to the vCenter Server system inventory during the evaluation period. After the evaluation period expires, you try to assign an edition license that limits the number of hosts that can be managed by a vCenter Server system. The assignment operation fails because the edition allows a vCenter Server system to manage fewer than 10 hosts. To correct this issue, you can upgrade your license key to a higher edition or you can remove hosts from the inventory.

As another example, if you configure a cluster of hosts to use Fault Tolerance and DRS during the evaluation period, you can only assign a license that allows the use of those features. Hence, the assignment of a higher edition license succeeds. To assign a lower edition license, you must first disable Fault Tolerance and DRS.

Access to the Licensing Reporting Manager

You cannot access the Licensing Reporting Manager.

Problem

You select **Home > Administration > Licensing Reporting Manager** from the vSphere Client Home page and nothing happens.

Cause

You might not be able to access the Licensing Reporting Manager because of one of the following reasons:

- Required services are not running.
- The Licensing Reporting Manager was not loaded properly as a plug-in to the vSphere Client.

Solution

Check the following services or areas of vCenter Server or the vSphere Client.

- Make sure that the VMware VirtualCenter Management Webservices Windows service is running on the vCenter Server instance.
- The Licensing Reporting Manager is a plug-in to the vSphere Client. Make sure that there are no errors for the Licensing Reporting Manager in the Plug-in Manager view.

Failure to Download Licensing Report

You cannot download the licensing report from the Licensing Reporting Manager.

Problem

You click **Download report** for a licensing report in the Licensing Reporting Manager, and the following error appears:

```
Cannot export license usage. License data integrity problem detected in the database
```

Cause

The license usage data stored in the database has been modified. Modifying license records in vCenter Server database is not recommended.

Solution

None. You can no longer download licensing reports for this vCenter Server or Linked Mode group with this time period.

Managing Users, Groups, Roles, and Permissions

8

Defining users, groups, roles, and permissions lets you control who has access to your vSphere managed objects and what actions they can perform.

vCenter Server and ESX/ESXi hosts determine the level of access for the user based on the permissions that you assign to the user. The combination of user name, password, and permissions is the mechanism by which vCenter Server and ESX/ESXi hosts authenticate a user for access and authorize the user to perform activities. The servers and hosts maintain lists of authorized users and the permissions assigned to each user.

Privileges define individual rights that are required for a user to perform actions and read properties. ESX/ESXi and vCenter Server use sets of privileges, or roles, to control which users or groups can access particular vSphere objects. ESX/ESXi and vCenter Server provide a set of preestablished roles. You can also create roles.

The privileges and roles assigned on an ESX/ESXi host are separate from the privileges and roles assigned on a vCenter Server system. When you manage a host using vCenter Server, only the privileges and roles assigned through the vCenter Server system are available. If you connect directly to the host using the vSphere Client, only the privileges and roles assigned directly on the host are available.

This chapter includes the following topics:

Managing vSphere Users

Several users can access the vCenter Server system from different vSphere Client sessions at the same time. vSphere does not explicitly restrict users with the same authentication credentials from accessing and taking action within the vSphere environment simultaneously.

A user is an individual authorized to log in to a host or vCenter Server.

You manage users defined on the vCenter Server system and users defined on individual hosts separately. Even if the user lists of a host and a vCenter Server system appear to have common users (for instance, a user called devuser), treat these users as separate users who have the same name. The attributes of devuser in vCenter Server, including permissions, passwords, and so forth, are separate from the attributes of devuser on the ESX/ESXi host. If you log in to vCenter Server as devuser, you might have permission to view and delete files from a datastore. If you log in to an ESX/ESXi host as devuser, you might not have these permissions.

vCenter Server Users

Authorized users for vCenter Server are those included in the Windows domain list referenced by vCenter Server or local Windows users on the vCenter Server system. The permissions defined for these users apply whenever a user connects to vCenter Server.

You cannot use vCenter Server to manually create, remove, or otherwise change vCenter Server users. To manipulate the user list or change user passwords, use the same tools that you use to manage your Windows domain or Active Directory. For more information about creating users and groups for use with vCenter Server, see your Microsoft documentation.

Changes that you make to the Windows domain are reflected in vCenter Server. Because you cannot directly manage users in vCenter Server, the user interface does not provide a user list for you to review. You see these changes only when you select users to configure permissions.

vCenter Servers connected in a Linked Mode group use Active Directory to maintain the list of users, allowing all vCenter Server systems in the group to share a common set of users.

Host Users

Users authorized to work directly on an ESX/ESXi host are added to the internal user list by default when ESX/ESXi is installed or by a system administrator after installation.

If you log in to an ESX/ESXi host as root using the vSphere Client, you can use the **Users and Groups** tab to perform management activities for these users. You can add users, remove users, change passwords, set group membership, and configure permissions.

You can also use Active Directory to manage users and groups for an ESX/ESXi host.

CAUTION See the Authentication and User Management chapter of the *ESX Configuration Guide* or *ESXi Configuration Guide* for information about root users and your ESX/ESXi host before you make any changes to the default users. Mistakes regarding root users can have serious access consequences.

Each ESX/ESXi host has two default users:

root user — The root user has full administrative privileges. Administrators use this log in and its associated password to log in to a host through the vSphere Client. Root users have a complete range of control activities on the specific host that they are logged on to, including manipulating permissions, creating groups and users (on ESX/ESXi hosts only), working with events, and so on.

vpxuser — The vpxuser user is a vCenter Server entity with root rights on the ESX/ESXi host, allowing it to manage activities for that host. The vpxuser is created at the time that an ESX/ESXi host is attached to vCenter Server. It is not present on the ESX host unless the host is being managed through vCenter Server.

NOTE You cannot manage vpxuser with Active Directory.

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).

Prerequisites

Verify that the vSphere Client is connected to a vCenter Server system or to the host.

Procedure

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

2 Under Software, select **Authentication Services** and click **Properties**.

3 In the Directory Services Configuration dialog box, select the type of authentication from the drop-down menu.

Option	Description
If you select Active Directory	Enter a domain in the form of **`name.tld`** or **`name.tld/container/path`** and click **Join Domain**.
If the host is already using a directory service	Select **Leave Domain** to leave the domain and join another.

4 Enter the user name and password of an Active Directory user who has permissions to join the host to the domain, and click **OK**.

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

Groups

You can manage some user attributes by creating groups. A group is a set of users that you manage through a common set of permissions.

A user can be a member of more than one group. When you assign permissions to a group, all users in the group inherit those permissions. Using groups can reduce the time it takes to set up your permissions model.

The group lists in vCenter Server and an ESX/ESXi host come from the same sources as the user lists. If you are working through vCenter Server, the group list is called from the Windows domain. If you are logged on to an ESX/ESXi host directly, the group list is called from a table maintained by the host.

Create groups for the vCenter Server system through the Windows domain or Active Directory database. Create groups for ESX/ESXi hosts using the Users and Groups tab in the vSphere Client when connected directly to the host.

NOTE If you use Active Directory groups, make sure that they are security groups and not distribution groups. Permissions assigned to distribution groups are not enforced by vCenter Server. For more information about security groups and distribution groups, see the Microsoft Active Directory documentation.

Removing or Modifying Users and Groups

When you remove users or groups, you also remove permissions granted to those users or groups. Modifying a user or group name causes the original name to become invalid.

See the Security chapter in the *ESX Configuration Guide* or *ESXi Configuration Guide* for information about removing users and groups from an ESX/ESXi host.

To remove users or groups from vCenter Server, you must remove them from the domain or Active Directory users and groups list.

If you remove users from the vCenter Server domain, they lose permissions to all objects in the vSphere environment and cannot log in again.

NOTE Users who are logged in and are removed from the domain keep their vSphere permissions until the next validation period. The default is every 24 hours.

Removing a group does not affect the permissions granted individually to the users in that group or permissions granted as part of inclusion in another group.

If you change a user's name in the domain, the original user name becomes invalid in the vCenter Server system. If you change the name of a group, the original group becomes invalid after you restart the vCenter Server system.

Best Practices for Users and Groups

Use best practices for managing users and groups to increase the security and manageability of your vSphere environment.

VMware recommends several best practices for creating users and groups in your vSphere environment:

- Use vCenter Server to centralize access control, rather than defining users and groups on individual hosts.
- Choose a local Windows user or group to have the Administrator role in vCenter Server.
- Create new groups for vCenter Server users. Avoid using Windows built-in groups or other existing groups.

Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define individual rights that a user requires to perform actions and read properties.

When you assign a user or group permissions, you pair the user or group with a role and associate that pairing with an inventory object. A single user might have different roles for different objects in the inventory. For example, if you have two resource pools in your inventory, Pool A and Pool B, you might assign a particular user the Virtual Machine User role on Pool A and the Read Only role on Pool B. These assignments would allow that user to turn on virtual machines in Pool A, but not those in Pool B. The user would still be able to view the status of the virtual machines in Pool B.

The roles created on an ESX/ESXi host are separate from the roles created on a vCenter Server system. When you manage a host using vCenter Server, the roles created through vCenter Server are available. If you connect directly to the host using the vSphere Client, the roles created directly on the host are available.

vCenter Server and ESX/ESXi hosts provide default roles:

System roles System roles are permanent. You cannot edit the privileges associated with these roles.

Sample roles VMware provides sample roles for convenience as guidelines and suggestions. You can modify or remove these roles.

You can also create roles.

All roles permit the user to schedule tasks by default. Users can schedule only tasks they have permission to perform at the time the tasks are created.

NOTE Changes to permissions and roles take effect immediately, even if the users involved are logged in. The exception is searches, where permission changes take effect after the user has logged out and logged back in.

Default Roles for ESX/ESXi and vCenter Server

vCenter Server, ESX, and ESXi provide default roles. These roles group privileges for common areas of responsibility in a vSphere environment.

You can use the default roles to assign permissions in your environment, or use them as a model to develop your own roles.

Table 8-1 lists the default roles for ESX/ESXi and vCenter Server.

Table 8-1. Default Roles

Role	Role Type	Description of User Capabilities
No Access	system	Cannot view or change the assigned object. vSphere Client tabs associated with an object appear without content. Can be used to revoke permissions that would otherwise be propagated to an object from a parent object. Available in ESX/ESXi and vCenter Server.
Read Only	system	View the state and details about the object. View all the tab panels in the vSphere Client except the Console tab. Cannot perform any actions through the menus and toolbars. Available on ESX/ESXi and vCenter Server.
Administrator	system	All privileges for all objects. Add, remove, and set access rights and privileges for all the vCenter Server users and all the virtual objects in the vSphere environment. Available in ESX/ESXi and vCenter Server.
Virtual Machine Power User	sample	A set of privileges to allow the user to interact with and make hardware changes to virtual machines, as well as perform snapshot operations. Privileges granted include: ■ All privileges for the scheduled task privileges group. ■ Selected privileges for global items, datastore, and virtual machine privileges groups. ■ No privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups. Usually granted on a folder that contains virtual machines or on individual virtual machines. Available on vCenter Server.

Table 8-1. Default Roles (Continued)

Role	Role Type	Description of User Capabilities
Virtual Machine User	sample	A set of privileges to allow the user to interact with a virtual machine's console, insert media, and perform power operations. Does not grant privileges to make virtual hardware changes to the virtual machine. Privileges granted include: ■ All privileges for the scheduled tasks privileges group. ■ Selected privileges for the global items and virtual machine privileges groups. ■ No privileges for the folder, datacenter, datastore, network, host, resource, alarms, sessions, performance, and permissions privileges groups. Usually granted on a folder that contains virtual machines or on individual virtual machines. Available on vCenter Server.
Resource Pool Administrator	sample	A set of privileges to allow the user to create child resource pools and modify the configuration of the children, but not to modify the resource configuration of the pool or cluster on which the role was granted. Also allows the user to grant permissions to child resource pools, and assign virtual machines to the parent or child resource pools. Privileges granted include: ■ All privileges for folder, virtual machine, alarms, and scheduled task privileges groups. ■ Selected privileges for resource and permissions privileges groups. ■ No privileges for datacenter, network, host, sessions, or performance privileges groups. Additional privileges must be granted on virtual machines and datastores to allow provisioning of new virtual machines. Usually granted on a cluster or resource pool. Available on vCenter Server.
VMware Consolidated Backup User	sample	Used by the VMware Consolidated Backup product. Do not modify. Available on vCenter Server.
Datastore Consumer	sample	A set of privileges to allow the user to consume space on the datastores on which this role is granted. To perform a space-consuming operation, such as creating a virtual disk or taking a snapshot, the user must also have the appropriate virtual machine privileges granted for these operations. Usually granted on a datastore or a folder of datastores. This role is available on vCenter Server.
Network Consumer	sample	A set of privileges to allow the user to assign virtual machines or hosts to networks, if the appropriate permissions for the assignment are also granted on the virtual machines or hosts. Usually granted on a network or folder of networks. Available on vCenter Server.

Create a Role

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

If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

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.

If you create or modify a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

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.

If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. However, assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

Procedure

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

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

3 Select **Administration > Role > Edit Role**.

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

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 to vCenter Server.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

If you remove a role from a vCenter Server system that is part of a connected group in Linked Mode, check the use of that role on the other vCenter Server systems in the group. Removing a role from one vCenter Server system removes the role from all other vCenter Server systems in the group, even if you reassign permissions to another role on the current vCenter Server system.

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.

Rename a Role

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

If you create or modify a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

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.

Permissions in vSphere

In vSphere, a permission consists of a user or group and an assigned role for an inventory object, such as a virtual machine or ESX/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 an ESX/ESXi host, a user must be granted a role that includes the **Host.Configuration.Memory Configuration** privilege. By assigning different roles to users or groups for different objects, you can control the tasks that users can perform in your vSphere environment.

By default, all users who are members of the Windows Administrators group on the vCenter Server system have the same access rights as a user assigned to the Administrator role on all objects. When connecting directly to an ESX/ESXi host, 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:

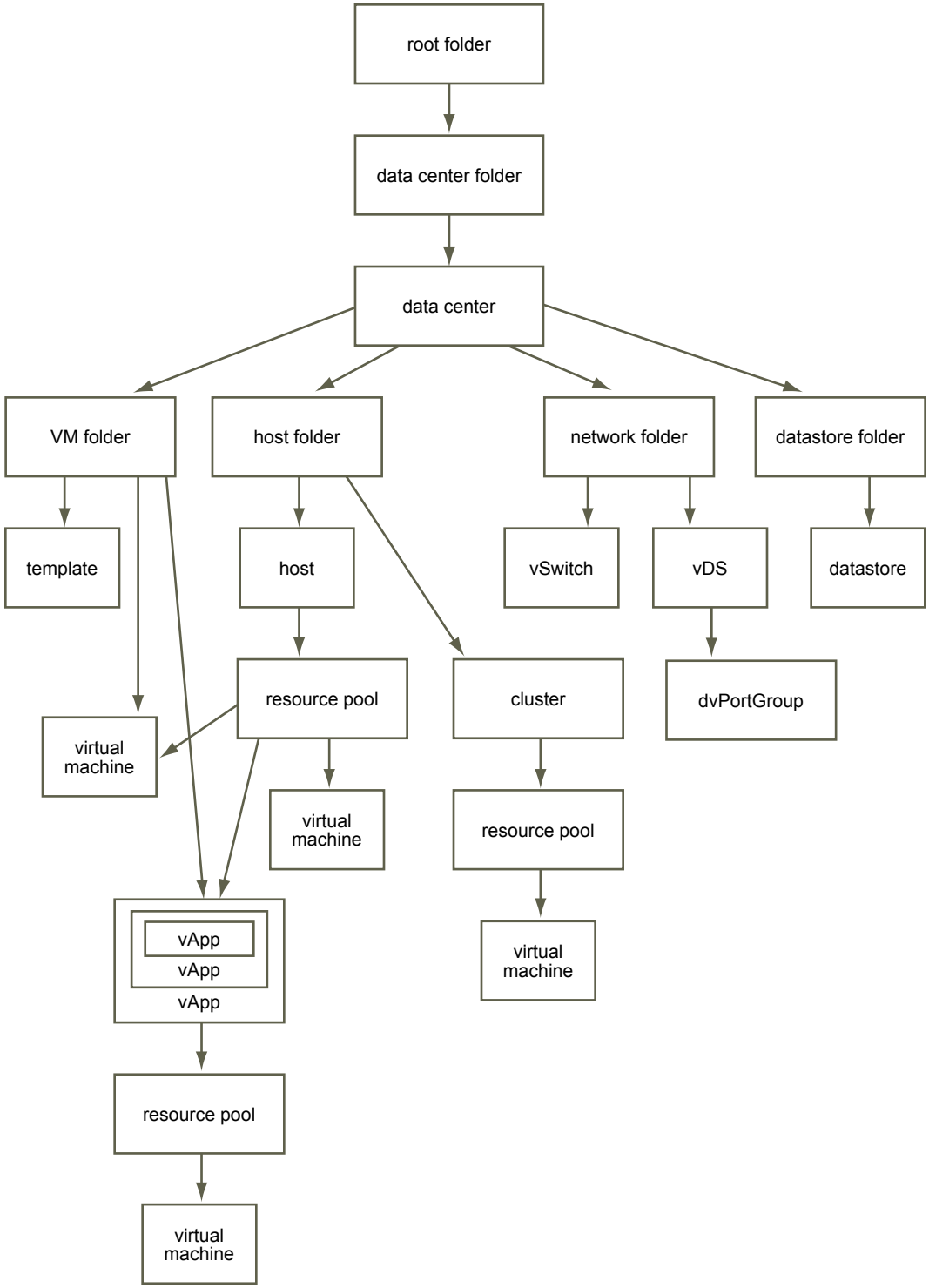
- Any operation that consumes storage space, such as creating a virtual disk or taking a snapshot, requires the **Datastore.Allocate Space** privilege on the target datastore, as well as the privilege to perform the operation itself.
- Moving an object in the inventory hierarchy requires appropriate 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.

Hierarchical Inheritance of Permissions

When you assign a permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission. Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

Figure 8-1 illustrates the vSphere inventory hierarchy and the paths by which permissions can propagate.

Figure 8-1. vSphere Inventory Hierarchy



Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent datacenter. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously. To restrict a user's privileges on a virtual machine, you must set permissions on both the parent folder and the parent host, cluster, or resource pool for that virtual machine.

To set permissions for a vNetwork Distributed Switch and its associated dvPort Groups, set permissions on a parent object, such a folder or datacenter. You must also select the option to propagate these permissions to child objects.

Permissions take several forms in the hierarchy:

Managed entities

You can define permissions on managed entities.

- Clusters
- Datacenters
- Datastores
- Folders
- Hosts
- Networks (except vNetwork Distributed Switches)
- dvPort Groups
- Resource pools
- Templates
- Virtual machines
- vApps

Global entities

Global entities derive permissions from the root vCenter Server system.

- Custom fields
- Licenses
- Roles
- Statistics intervals
- Sessions

Multiple Permission Settings

Objects might have multiple permissions, but only one permission for each user or group.

Permissions applied on a child object always override permissions that are applied on a parent object. Virtual machine folders and resource pools are equivalent levels in the hierarchy. If you assign propagating permissions to a user or group on a virtual machine's folder and its resource pool, the user has the privileges propagated from the resource pool and from the folder.

If multiple group permissions are defined on the same object and the user belongs to two or more of those groups, two situations are possible:

- If no permission is defined for the user on that object, the user is assigned the set of privileges assigned to the groups for that object.
- If a permission is defined for the user on that object, the user's permission takes precedence over all group permissions.

Example 1: Inheritance of Multiple Permissions

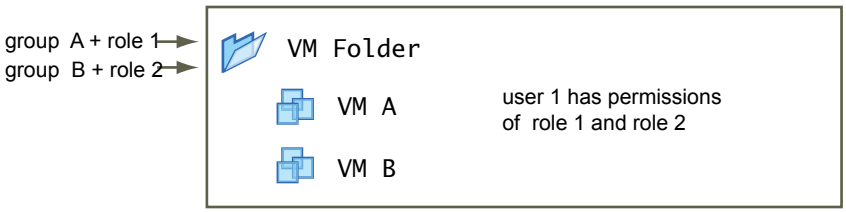
This example illustrates how an object can inherit multiple permissions from groups that are granted permission on a parent object.

In this example, two permissions are assigned on the same object for two different groups.

- Role 1 can power on virtual machines.
- Role 2 can take snapshots of virtual machines.
- Group A is granted Role 1 on VM Folder, with the permission set to propagate to child objects.
- Group B is granted Role 2 on VM Folder, with the permission set to propagate to child objects.
- User 1 is not assigned specific permission.

User 1, who belongs to groups A and B, logs on. User 1 can both power on and take snapshots of VM A and VM B.

Figure 8-2. Example 1: Inheritance of Multiple Permissions



Example 2: Child Permissions Overriding Parent Permissions

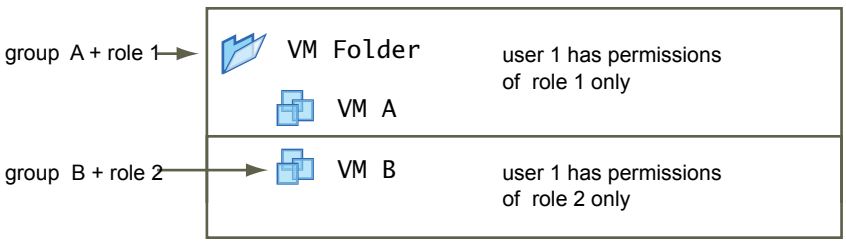
This example illustrates how permissions that are assigned on a child object can override permissions that are assigned on a parent object. You can use this overriding behavior to restrict user access to particular areas of the inventory.

In this example, permissions are assigned to two different groups on two different objects.

- Role 1 can power on virtual machines.
- Role 2 can take snapshots of virtual machines.
- Group A is granted Role 1 on VM Folder, with the permission set to propagate to child objects.
- Group B is granted Role 2 on VM B.

User 1, who belongs to groups A and B, logs on. Because Role 2 is assigned at a lower point in the hierarchy than Role 1, it overrides Role 1 on VM B. User 1 can power on VM A, but not take snapshots. User 1 can take snapshots of VM B, but not power it on.

Figure 8-3. Example 2: Child Permissions Overriding Parent Permissions



Example 3: User Permissions Overriding Group Permissions

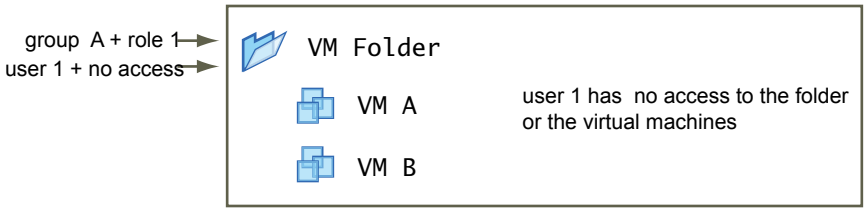
This example illustrates how permissions assigned directly to an individual user override permissions assigned to a group that the user is a member of.

In this example, permissions are assigned to a user and to a group on the same object.

- Role 1 can power on virtual machines.
- Group A is granted Role 1 on VM Folder.
- User 1 is granted No Access role on VM Folder.

User 1, who belongs to group A, logs on. The No Access role granted to User 1 on VM Folder overrides the group permission. User 1 has no access to VM Folder or VMs A and B.

Figure 8-4. Example 3: User Permissions Overriding Group Permissions



Permission Validation

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

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

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

Assign Permissions

After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same permissions at one time on multiple objects by moving the objects to a folder and setting the permissions on the folder.

Prerequisites

Permissions.Modify permission on the parent object of the object whose permissions you want to modify.

Procedure

1 Select an object and click the **Permissions** tab.

2 Right-click the **Permissions** tab and select **Add Permission**.

3 Select a role from the **Assigned Role** drop-down menu.

The roles that are assigned to the object appear in the menu. The privileges contained in the role are listed in the section below the role title.

4 (Optional) Deselect the **Propagate to Child Objects** check box.

The role is applied only to the selected object, and does not propagate to the child objects.

5 Click **Add** to open the Select Users or Groups dialog box.

6 Identify the user or group to assign to this role.

a Select the domain where the user or group is located from the **Domain** drop-down menu.

b Type a name in the Search box or select a name from the **Name** list.

c Click **Add**.

The name is added to either the **Users** or **Groups** list.

d Repeat Step 6a through Step 6c to add additional users or groups.

e Click **OK** when finished.

7 Verify that the users and groups are assigned to the appropriate permissions and click **OK**.

8 Click **OK** to finish.

The server adds the permission to the list of permissions for the object.

The list of permissions references all users and groups that have roles assigned to the object, and indicates where in the vCenter Server hierarchy the role is assigned.

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. ESX/ESXi user lists cannot be searched in the same way.

Procedure

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

2 Click the **Active Directory** item.

3 Change the values as needed.

Option	Description
Active Directory Timeout	Specifies in seconds the maximum amount of time vCenter Server allows the search to run on the selected domain. Searching large domains can take a long time.
Enable Query Limit	To set no maximum limit on the number of users and groups that vCenter Server displays from the selected domain, deselect the check box.
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.

4 Click **OK**.

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 Management Server Configuration**.

2 Click the **Active Directory** list item.

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.

Change Permissions

After a user or group and role pair is set for an inventory object, you can change the role paired with the user or group 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 Click the line item to select the user or group and role pair.

4 Select **Inventory > Permissions > Properties**.

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

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

Remove Permissions

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

Procedure

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

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

3 Click the **Permissions** tab.

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

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

vCenter Server removes the permission setting.

Best Practices for Roles and Permissions

Use best practices for roles and permissions to maximize the security and manageability of your vCenter Server environment.

VMware recommends the following best practices when configuring roles and permissions in your vCenter Server environment:

- Where possible, grant permissions to groups rather than individual users.
- Grant permissions only where needed. Using the minimum number of permissions makes it easier to understand and manage your permissions structure.

- If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges. Otherwise, you could unintentionally restrict administrators' privileges in parts of the inventory hierarchy where you have assigned that group the restrictive role.
- Use folders to group objects to correspond to the differing permissions you want to grant for them.
- Use caution when granting a permission at the root vCenter Server level. Users with permissions at the root level have access to global data on vCenter Server, such as roles, custom attributes, vCenter Server settings, and licenses. Changes to licenses and roles propagate to all vCenter Server systems in a Linked Mode group, even if the user does not have permissions on all of the vCenter Server systems in the group.
- In most cases, enable propagation on permissions. This ensures that when new objects are inserted in to the inventory hierarchy, they inherit permissions and are accessible to users.
- Use the No Access role to masks specific areas of the hierarchy that you don't want particular users to have access to.

Required Privileges for Common Tasks

Many tasks require permissions on more than one object in the inventory. You can review the privileges required to perform the tasks and, where applicable, the appropriate sample roles.

Table 8-2 lists common tasks that require more than one privilege. You can use the Applicable Roles on the inventory objects to grant permission to perform these tasks, or you can create your own roles with the equivalent required privileges.

Table 8-2. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or datacenter: ■ **Virtual Machine.Inventory.Create** ■ **Virtual Machine.Configuration.Add New Disk** (if creating a new virtual disk) ■ **Virtual Machine .Configuration.Add Existing Disk** (if using an existing virtual disk) ■ **Virtual Machine.Configuration.Raw Device** (if using a RDM or SCSI pass-through device)	Virtual Machine Administrator
	On the destination host, cluster, or resource pool: **Resource.Assign Virtual Machine to Resource Pool**	Virtual Machine Administrator
	On the destination datastore or folder containing a datastore: **Datastore.Allocate Space**	Datastore Consumer or Virtual Machine Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign Network**	Network Consumer or Virtual Machine Administrator
Deploy a virtual machine from a template	On the destination folder or datacenter: ■ **Virtual Machine.Inventory.Create** ■ **Virtual Machine.Configuration.Add New Disk**	Virtual Machine Administrator
	On a template or folder of templates: **Virtual Machine.Provisioning.Deploy Template**	Virtual Machine Administrator
	On the destination host, cluster or resource pool: **Resource.Assign Virtual.Machine to Resource Pool**	Virtual Machine Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate Space**	Datastore Consumer or Virtual Machine Administrator

Table 8-2. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
	On the network that the virtual machine will be assigned to: **Network.Assign Network**	Network Consumer or Virtual Machine Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual Machine.State.Create Snapshot**	Virtual Machine Power User or Virtual Machine Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate Space**	Datastore Consumer or Virtual Machine Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: ■ **Resource.Assign Virtual Machine to Resource Pool** ■ **Virtual Machine.Inventory.Move**	Virtual Machine Administrator
	On the destination resource pool: **Resource.Assign Virtual Machine to Resource Pool**	Virtual Machine Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: ■ **Virtual Machine.Interaction.Answer Question** ■ **Virtual Machine.Interaction.Console Interaction** ■ **Virtual Machine.Interaction.Device Connection** ■ **Virtual Machine.Interaction.Power Off** ■ **Virtual Machine.Interaction.Power On** ■ **Virtual Machine.Interaction.Reset** ■ **Virtual Machine.Interaction.Configure CD Media** (if installing from a CD) ■ **Virtual Machine.Interaction.Configure Floppy Media** (if installing from a floppy disk) ■ **Virtual Machine.Interaction.Tools Install**	Virtual Machine Power User or Virtual Machine Administrator
	On a datastore containing the installation media ISO image: **Datastore.Browse Datastore** (if installing from an ISO image on a datastore)	Virtual Machine Power User or Virtual Machine Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate** ■ **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign Virtual Machine to Resource Pool**	Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: ■ **Resource.Relocate** ■ **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign Virtual Machine to Resource Pool**	Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator
	On the destination datastore (if different from the source): **Datastore.Allocate Space**	Datastore Consumer or Virtual Machine Administrator

Table 8-2. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Migrate a Virtual Machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource.Migrate**	Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator
	On the destination datastore: **Datastore.Allocate Space**	Datastore Consumer or Virtual Machine Administrator
Move a host into a cluster	On the host: **Host.Inventory.Add Host to Cluster**	Datacenter Administrator or Virtual Machine Administrator
	On the destination cluster: **Host.Inventory.Add Host to Cluster**	Datacenter Administrator or Virtual Machine Administrator

Monitoring Your Virtual Infrastructure

Working with Performance Statistics 9

You can configure how statistics are collected and archived for your vCenter Server system. This configuration determines the data available in the performance charts, which you use to monitor and troubleshoot performance in your virtual environment.

This chapter includes the following topics:

Statistics Collection for vCenter Server

The performance data collection subsystem for vSphere collects performance data on a variety of inventory items and their devices. Data counters define individual performance metrics. Performance metrics are organized into logical groups based on the object or object device. Statistics for one or more metrics can be displayed in a chart. The data collection subsystem is configurable. You can adjust the duration of collection intervals and the amount of data collected for an interval. You can also customize charts by adding or removing data counters.

Table 9-1 lists each metric group and describes the type of data collected.

Table 9-1. Metric Groups

Metric group	Description
Cluster Services	Performance statistics for clusters configured by using VMware DRS (distributed resource scheduler), VMware HA (high availability), or both.
CPU	CPU utilization per host, virtual machine, resource pool, or compute resource.
Datastore	Statistics for datastore utilization
Disk	Disk utilization per host, virtual machine, or datastore. Disk metrics include I/O performance (such as latency and read/write speeds), and utilization metrics for storage as a finite resource.
Management Agent	Memory swap statistics per COS.
Memory	Memory utilization per host, virtual machine, resource pool, or compute resource. The value obtained is one of the following: ■ For virtual machines, memory refers to guest physical memory. Guest physical memory is the amount of physical memory presented as a virtual-hardware component to the virtual machine, at creation time, and made available when the virtual machine is running. ■ For hosts, memory refers to machine memory. Machine memory is the RAM that is installed in the hardware that comprises the ESX/ESXi system.

Table 9-1. Metric Groups (Continued)

Metric group	Description
Network	Network utilization for both physical and virtual network interface controllers (NICs) and other network devices, such as the virtual switches (vSwitch) that support connectivity among all components (hosts, virtual machines, VMkernel, and so on).
Power	Energy usage statistics per host.
Storage Adapter	Data traffic statistics per HBA.
Storage Path	Data traffic statistics per path.
System	Overall system availability, such as system heartbeat and uptime. These counters are available directly from ESX and from vCenter Server.
Virtual Machine Operations	Virtual machine power and provisioning operations in a cluster or datacenter.

For more information about available statistics, see the *vSphere API Reference*.

Data Counters

vCenter Server and ESX/ESXi hosts use data counters to query for statistics. A data counter is a unit of information relevant to a given object.

For example, network metrics for a virtual machine include one counter that tracks the rate at which data is transmitted and another counter that tracks the rate at which data is received across a NIC instance.

To ensure performance is not impaired when collecting and writing the data to the database, cyclical queries are used to collect data counter statistics. The queries occur for a specified collection interval. At the end of each interval, the data calculation occurs.

Each data counter includes several attributes that are used to determine the statistical value collected. Table 9-2 lists data counter attributes.

Table 9-2. Data Counter Attributes

Attribute	Description
Unit of Measurement	Standard in which the statistic quantity is measured. ■ Kilobytes (KB) – 1024 bytes ■ Kilobytes per second (KBps) – 1024 bytes per second ■ Kilobits (kb) – 1000 bits ■ Kilobits per second (kbps) – 1000 bits per second ■ Megabytes (MB) ■ megabytes per second (MBps) ■ megabits (Mb), megabits per second (Mbps) ■ megahertz (MHz) ■ microseconds (μs) ■ milliseconds (ms) ■ number (#) ■ percent (%) ■ seconds (s)
Description	Text description of the data counter.
Statistics Type	Measurement used during the statistics interval. Related to the unit of measurement. ■ Rate – Value over the current statistics interval ■ Delta – Change from previous statistics interval. ■ Absolute – Absolute value (independent of the statistics interval).

Table 9-2. Data Counter Attributes (Continued)

Attribute	Description
Rollup Type	Calculation method used during the statistics interval to roll up data. Determines the type of statistical values that are returned for the counter. ■ Average – Data collected during the interval is aggregated and averaged. ■ Minimum – The minimum value is rolled up. ■ Maximum – The maximum value is rolled up. The Minimum and Maximum values are collected and displayed only in statistics level 4. Minimum and maximum rollup types are used to capture peaks in data during the interval. For real-time data, the value is the current minimum or current maximum. For historical data, the value is the average minimum or average maximum. For example, the following information for the CPU usage chart shows that the average is collected at statistics level 1 and the minimum and maximum values are collected at statistics level 4. ■ Counter: usage ■ Unit: Percentage (%) ■ Rollup Type: Average (Minimum/Maximum) ■ Collection Level: 1 (4) ■ Summation – Data collected is summed. The measurement displayed in the chart represents the sum of data collected during the interval. ■ Latest – Data collected during the interval is a set value. The value displayed in the performance charts represents the current value.
Collection level	Number of data counters used to collect statistics. Collection levels range from 1 to 4, with 4 having the most counters.

Collection Intervals

Collection intervals determine the time period during which statistics are aggregated and rolled up, and the length of time the statistics are archived in the vCenter database.

By default, vCenter Server has four collection intervals: **Day**, **Week**, **Month**, and **Year**. Each interval specifies a length of a time statistics are archived in the vCenter database. You can configure which intervals are enabled and for what period of time. You can also configure the number of data counters used during a collection interval by setting the collection level. Together, the collection interval and collection level determine how much statistical data is collected and stored in your vCenter Server database.

Real-time statistics are not stored in the database. They are stored in a flat file on ESX/ESXi hosts and in memory on the vCenter Server systems. ESX/ESXi hosts collect real-time statistics only for the host or the virtual machines available on the host. Real-time statistics are collected directly on an ESX/ESXi host every 20 seconds (60 seconds for ESX Server 2.x hosts). If you query for real-time statistics in the vSphere Client for performance charts, vCenter Server queries each host directly for the data. It does not process the data at this point. It only passes the data to the vSphere Client. The processing occurs in a separate operation. On ESX/ESXi hosts, the statistics are kept for one hour, after which 180 data points (15 -20 second samples) will have been collected. The data points are aggregated, processed, and returned to vCenter Server. At this point, vCenter Server archives the data in the database as a data point for the **Day** collection interval.

To ensure performance is not impaired when collecting and writing the data to the database, cyclical queries are used to collect data counter statistics. The queries occur for a specified collection interval. At the end of each interval, the data calculation occurs.

Table 9-3 lists the default collection intervals available for the vCenter Server.

Table 9-3. Collection Intervals

Collection Interval/Archive Length	Collection Frequency	Default Behavior
1 Day	5 Minutes	Real-time statistics are rolled up to create one data point every 5 minutes. The result is 12 data points every hour and 288 data points every day. After 30 minutes, the six data points collected are aggregated and rolled up as a data point for the 1 Week time range. You can change the interval duration and archive length of the 1 Day collection interval by configuring the statistics settings.
1 Week	30 Minutes	1 Day statistics are rolled up to create one data point every 30 minutes. The result is 48 data points every day and 336 data points every week. Every 2 hours, the 12 data points collected are aggregated and rolled up as a data point for the 1 Month time range. You cannot change the default settings of the 1 Week collection interval.
1 Month	2 Hours	1 Week statistics are rolled up to create one data point every 2 hours. The result is 12 data points every day and 360 data points every month (assuming a 30-day month). After 24 hours, the 12 data points collected are aggregated and rolled up as a data point for the **1 Year** time range. You cannot change the default settings of the 1 Month collection interval.
1 Year	1 Day	1 Month statistics are rolled up to create one data point every day. The result is 365 data points each year. You can change the interval duration and archive length of the 1 Year collection interval by configuring the statistics settings.

Configure Collection Intervals

You can change the frequency at which statistic queries occur, the length of time statistical data is stored in the vCenter Server database, and the amount of statistical data collected. By default, all collection intervals are enabled and query for statistics at statistics level 1.

Prerequisites

To configure statistics settings, verify that the vSphere Client is connected to a vCenter Server system.

NOTE Not all attributes are configurable for each collection interval.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 If your environment uses multiple vCenter Servers, in **Current vCenter Server**, select the server.

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

4 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. If you disable all collection intervals, statistical data is not archived in the vCenter Server database.

5 (Optional) To change a collection interval attribute, select its row in the Statistics Interval section and click **Edit**.

   a In **Keep Samples for**, select an archive length for the Day and Year intervals.

   b In **Statistics Interval**, select an interval duration 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 preceding statistics interval. This is a vCenter Server dependency.

6 (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 (Optional) Make changes to your statistics collection settings.

7 Click **OK**.

Enable or Disable Collection Intervals

Enabling and disabling statistics intervals controls the amount of statistical data saved to the vCenter Server database.

Prerequisites

To configure statistics settings, verify that the vSphere Client is connected to a vCenter Server system.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 If your environment uses multiple vCenter Servers, in **Current vCenter Server**, select the appropriate server.

3 In the vCenter Server Settings dialog box, select **Statistics**.

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

   NOTE When you disable a collection interval, all subsequent intervals are automatically disabled.

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 (Optional) Make changes to your statistics collection settings.

6 Click **OK**.

Statistics Levels

Each collection interval has a default statistics level that determines how many data counters are used when you collect statistics data.

The statistics level establishes which metrics are retrieved and recorded in the vCenter Server database. You can assign a statistics level of 1- 4 to each collection interval, with level 4 having the largest number of counters. By default, all collection intervals use statistics level 1.

The statistics level for an interval cannot be greater than the statistics level set for the preceding collection interval. For example, if the Month interval is set to statistics level 3, the Year interval can be set to statistics level 1, 2, or 3, but not to statistics level 4. This is a vCenter Server dependency.

Table 9-4 describes each statistics level and provides recommendations on when to use them.

Table 9-4. Statistics Levels

Level	Metrics	Best Practice
Level 1	■ Cluster Services (VMware Distributed Resource Scheduler) – all metrics ■ CPU – cpuentitlement, totalmhz, usage (average), usagemhz ■ Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used ■ Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon) ■ Network – usage (average) ■ System – heartbeat, uptime ■ Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required. Level 1 is the default Collection Level for all Collection Intervals.
Level 2	■ Level 1 metrics ■ CPU – idle, reservedCapacity ■ Disk – All metrics, excluding numberRead and numberWrite. ■ Memory – All metrics, excluding memUsed and maximum and minimum rollup values. ■ Virtual Machine Operations – All metrics	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.
Level 3	■ Level 1 and Level 2 metrics ■ Metrics for all counters, excluding minimum and maximum rollup values. ■ Device metrics	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 3 for the shortest time period (Day or Week collection interval).
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 4 for the shortest amount of time.

Generally, you use only statistics levels 1 and 2 for performance monitoring and analysis. Levels 3 and 4 provide granularity that is useful only for developers. Unless vCenter Server is set to a statistics level that contains a data counter, the data for that counter is not stored in the database nor is it rolled up into a past-day statistic on the ESX/ESXi host. The counter will not appear in the performance charts.

Using Collection Levels Effectively

Using statistics level 1 is adequate for monitoring performance. In some instances you might need to collect more performance statistics, for example, to troubleshoot performance problems.

Before you increase the statistics level for an interval, view charts in real time. Viewing real-time data has less impact on performance because metrics are retrieved directly from the source without being written to the vCenter Server database.

If you change to statistics level 3 or 4 to diagnose problems, reset the statistics level to its previous state as soon as possible. At statistics level 4, limit the collection period to the Day interval to not have an impact on the database. To save the data for longer than one day, increase the interval to two or three days rather than using the Week interval. For example, to record data over the weekend, set the interval to three days. Use a week interval only when you need the duration to be more than three days.

Table 9-5 lists the circumstances in which you might want to increase the statistics level for your vCenter Server.

Table 9-5. Collection Level Scenarios

Use Collection Level	To do this
2	■ Identify virtual machines that can be co-located because of complimentary memory sharing. ■ Detect the amount of active memory on a host to determine whether it can handle additional virtual machines.
3	■ Compare ready and wait times of virtual CPUs to determine the effectiveness of VSMP. ■ Diagnose problems with devices, or compare performance among multiple devices.
4	■ Determine whether a device is being saturated. ■ Troubleshoot errors.

How Metrics Are Stored in the vCenter Server Database

The metrics gathered for each collection interval are stored in their own database tables.

At the end of an interval, one of two things can occur.

- If the next interval is disabled, the data in the table that is older than the interval duration is purged.
- If the next interval is enabled, the data is aggregated into groups and is rolled up to the database table of the subsequent collection interval. For example, the day interval has a 5 minute collection frequency, and the week interval has a 30 minute collection frequency. When the day interval completes, it aggregates the 5 minute queries into groups of six (equaling 30 minutes) and rolls the 30-minute data block to the week interval database table. The day-old data is then purged from the database to make room for new queries.

You control how long statistical data is stored in the vCenter Server database by enabling or disabling a collection interval. When you disable a collection interval, all subsequent intervals are automatically disabled. For example, when you disable the week interval, the month and year intervals are also disabled. Data is purged at the end of the day interval cycle because no rollups can occur. The oldest data is purged first.

NOTE You must manually enable each collection interval to use it again. Also, you can only enable a collection interval if all previous statistics intervals are enabled. For example, to enable the month interval, the day and week intervals must be enabled.

By default, statistics are stored in the vCenter Server database for one year. You can increase this to three years. To save statistical data for longer than three years, archive it outside of the vCenter Server database.

Estimate the Statistics Impact on the vCenter Server Database

After you configure statistics intervals, you can verify that the vCenter Server database has enough space to archive the data collected.

Estimate the statistics effect in the vSphere Client.

Procedure

1 Open the **Statistics** tab of the vCenter Server Settings dialog box.

   a Select **Administration > vCenter Server Settings**.

   b In the navigation panel, click **Statistics**.

2 (Optional) Edit a statistics interval.

   a Select the interval to change.

   b Click **Edit**.

   c Change the settings as necessary.

   d Click **OK**.

3 Enter the number of physical hosts and virtual machines in your inventory.

   The vCenter Server uses a database calculator to determine the estimated size required for your statistics configuration. The value appears in the **Estimated space required** field after you enter values.

4 Click **OK**.

Statistics Collection for Microsoft Windows Guest Operating Systems

In a virtualized environment, physical resources are shared among multiple virtual machines.

Some virtualization processes dynamically allocate available resources depending on the status, or utilization rates, of virtual machines in the environment. This can make obtaining accurate information about the resource utilization (CPU utilization, in particular) of individual virtual machines, or applications running within virtual machines, difficult. VMware now provides virtual machine-specific performance counter libraries for the Windows Perfmon utility. Application administrators can view accurate virtual machine resource utilization statistics from within the guest operating system's Windows Perfmon utility.

Enable Statistics Collection for Guest Operating System Performance Analysis

VMware-specific performance objects are loaded into Microsoft Windows Perfmon and enabled when VMware Tools is installed.

To display a performance chart for any performance object, you must add counters. See "View Performance Statistics for Windows Guest Operating Systems," on page 116

View Performance Statistics for Windows Guest Operating Systems

You can display VMware specific statistics in the Microsoft Windows Perfmon utility.

Prerequisites

Verify that a virtual machine with a Microsoft Windows operating system and VMware Tools is installed.

Procedure

1 Open a console to the virtual machine and log in.

2 Select **Start > Run**.

3 Enter **Perfmon** and press **Enter**.

4 In the Performance dialog box, click **Add** .

5 In the Add Counters dialog box, select **Use local computer counters**.

6 Select a virtual machine performance object.

Virtual machine performance object names begin with **VM**.

7 Select the counters that you want to display for that object.

8 If the performance object has multiple instances, select the instances you want to display.

9 Click **Add**.

The Performance dialog box displays data for the selected performance object.

10 Click **Close** to close the Add Counter dialog box and return to the Performance dialog box.

vCenter Server Performance Charts

The performance charts graphically display CPU, memory, disk, network, and storage metrics for devices and entities managed by vCenter Server. Chart types include line charts, pie charts, bar charts, and stacked charts.

You view the performance charts for an object that is selected in the inventory on the vSphere Client **Performance** tab. You can view overview charts and advanced charts for an object. Both the overview charts and the advanced charts use the following chart types to display statistics.

Line charts Display metrics for a single inventory object. The data for each performance counter is plotted on a separate line in the chart. For example, a network chart for a host can contain two lines: one showing the number of packets received, and one showing the number of packets transmitted.

Bar charts Display storage metrics for datastores in a selected datacenter. Each datastore is represented as a bar in the chart, and each bar displays metrics based on file type (virtual disks, snapshots, swap files, and other files).

Pie charts Display storage metrics for a single datastore or virtual machine. Storage information is based on file type or virtual machine. For example, a pie chart for a datastore displays the amount of storage space occupied by the five-largest virtual machines on that datastore. A pie chart for a virtual machine displays the amount of storage space occupied by virtual machine files.

Stacked charts Display metrics for children of the selected parent object. For example, a host's stacked CPU usage chart displays CPU usage metrics for each virtual machine on the host. The metrics for the host itself are displayed in separate line charts. Stacked charts are useful in comparing resource allocation and usage across multiple hosts or virtual machines. Each metric group appears on a separate chart for a managed entity. For example, hosts have one chart that displays CPU metrics and one that displays memory metrics.

Overview Performance Charts

The overview performance charts enable you to view CPU, memory, network, disk, and storage metrics for an object at the same time.

All overview charts for an object appear in the same panel in the **Performance** tab. This allows you to do side-by-side comparisons of resource usage for clusters, datacenters, datastores, hosts, resource pools, and virtual machines. You can perform the following tasks with the overview performance charts.

- View all charts for an object in one panel. The single-panel view enables you to make side-by-side comparisons of different resource statistics, for example, CPU usage and memory usage.
- View real-time and historic data.
- View thumbnail charts for child objects. Thumbnail charts provide a quick summary of resource usage for each child object of a datacenter, datastore, cluster, or host.
- Open the overview charts for a child object by clicking the object name in the thumbnail section.

View the Overview Performance Charts

You can view CPU, memory, disk, network, and storage statistics for an object in the overview performance charts. These charts support a subset of data counters supported by vCenter Server.

Prerequisites

Verify that the vSphere Client is connected to a vCenter Server system.

Procedure

1 Select the inventory object and click the **Performance** tab.

2 Click **Overview**.

The overview charts for the object appear.

View the Overview Performance Charts Help

The Performance Chart Help contains information about how to work with overview charts, including how to analyze chart data and how to set the time range for the chart data. It also describes the metric counters displayed in each overview chart.

Procedure

1 Select the inventory object and click the **Performance** tab.

2 Click **Overview**.

3 Click the Help icon (**?**).

4 To view the Help for a specific chart, click the Help icon for that chart.

Advanced Performance Charts

With the advanced performance charts, you can see data point information for a plotted metric, export chart data to a spreadsheet, and save chart data to a file. You can customize the advanced chart views.

NOTE You cannot view datastore metrics in the advanced charts. They are available only in the overview charts.

View the Advanced Performance Charts

You can view CPU, memory, disk, and network statistics for an object in the advanced performance charts. These charts support data counters that are not supported in the overview performance charts.

When connected directly to an ESX/ESXi host, the advanced performance charts display only real-time statistics and past day statistics. To view historical data, the vSphere Client must be connected to a vCenter Server system.

Procedure

1 Select an inventory object.

2 Click the **Performance** tab.

3 Click **Advanced**.

4 To view a different chart, select an option from the **Switch to** list.

The amount of historical data displayed in a chart depends on the collection interval and statistics level set for vCenter Server.

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.

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. Use the vSphere Client to export data.

Prerequisites

Verify that the time is set correctly on the ESX/ESXi host, the vCenter Server system, and the client machine. Each host and client machine can be in different time zones, but the times must be correct for their respective time zones.

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 using the **All** or **None** buttons.

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.

Customize Advanced Chart Views

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 your own chart views.

Changes to chart options take effect immediately. New views are added to the **Switch to** menu.

Procedure

1 Select an inventory object and click the **Performance** tab.

2 Click **Advanced**.

3 Click **Chart Options**.

4 Select a metric group.

5 Select a time range.

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.

6 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.

7 In Objects, select the inventory objects to display in the chart.

You can also specify the objects using the **All** or **None** buttons.

8 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.

9 Click **Apply** to see the results.

10 Click **OK**.

To view the chart in its own window, click the pop-up chart button (). You can view additional charts while keeping this chart open.

Delete a Custom Advanced Chart View

You can delete custom chart views from the vSphere Client.

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**.

Monitoring and Troubleshooting Performance

You monitor CPU, memory, disk, network, and storage metrics by using the performance charts located on the **Performance** tab of the vSphere Client. Use the following guidelines to identify and resolve potential performance problems.

- CPU Performance on page 121

  Use the vSphere Client CPU performance charts to monitor CPU usage for hosts, clusters, resource pools, virtual machines, and vApps. Use the guidelines below to identify and correct problems with CPU performance.

- Disk I/O Performance on page 122

  Use the vSphere Client disk performance charts to monitor disk I/O usage for clusters, hosts, and virtual machines. Use the guidelines below to identify and correct problems with disk I/O performance.

- Memory Performance on page 123

  Use the vSphere Client memory performance charts to monitor memory usage of clusters, hosts, virtual machines, and vApps. Use the guidelines below to identify and correct problems with memory performance.

- Network Performance on page 124

  Use the network performance charts to monitor network usage and bandwidth for clusters, hosts, and virtual machines. Use the guidelines below to identify and correct problems with networking performance.

- Storage Performance on page 125

  Use the vSphere Client datastore performance charts to monitor datastore usage. Use the guidelines below to identify and correct problems with datastore performance.

CPU Performance

Use the vSphere Client CPU performance charts to monitor CPU usage for hosts, clusters, resource pools, virtual machines, and vApps. Use the guidelines below to identify and correct problems with CPU performance.

A short spike in CPU usage or CPU ready indicates that you are making the best use of the host resources. However, if both values are constantly high, the hosts are probably overcommitted. Generally, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is impacted.

Table 9-6. CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked bar chart on the host's **Virtual Machine** view shows the CPU usage for all virtual machines on the host.
3	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
4	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
5	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the ESX/ESXi host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
6	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
7	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
8	Upgrade the physical CPUs or cores on the host if necessary.
9	Use the newest version of ESX/ESXi, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Disk I/O Performance

Use the vSphere Client disk performance charts to monitor disk I/O usage for clusters, hosts, and virtual machines. Use the guidelines below to identify and correct problems with disk I/O performance.

The virtual machine disk usage (%) and I/O data counters provide information about average disk usage on a virtual machine. Use these counters to monitor trends in disk usage.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You use the Advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value should be 0-1 milliseconds. If the value is greater than 4ms, the virtual machines on the ESX/ESXi host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15ms indicates there are probably problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

Table 9-7. Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. This should allow for more operating system caching, which can reduce I/O activity. Note that this may require you to also increase the host memory. Increasing memory might reduce the need to store data because databases can utilize system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. Consider array-side improvements to increase throughput.
5	Use Storage VMotion to migrate I/O-intensive virtual machines across multiple ESX/ESXi hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see the *Fibre Channel SAN Configuration Guide*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. This alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's .VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current ESX/ESXi host hardware.

Memory Performance

Use the vSphere Client memory performance charts to monitor memory usage of clusters, hosts, virtual machines, and vApps. Use the guidelines below to identify and correct problems with memory performance.

To ensure best performance, the host memory must be large enough to accommodate the active memory of the virtual machines. Note that the active memory can be smaller than the virtual machine memory size. This allows you to over-provision memory, but still ensures that the virtual machine active memory is smaller than the host memory.

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation which may degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot handle the demand for memory. This leads to memory reclamation which may degrade performance.

If memory usage is high or you notice degredation in performance, consider taking the actions listed below.

Table 9-8. Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Network Performance

Use the network performance charts to monitor network usage and bandwidth for clusters, hosts, and virtual machines. Use the guidelines below to identify and correct problems with networking performance.

Network performance is dependent on application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

NOTE In some instances, large packets can result in high network latency. To check network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

Table 9-9. Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same ESX/ESXi host communicate with each other, connect them to the same vSwitch to avoid the cost of transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, VMotion tasks, and service console activities.

Table 9-9. Networking Performance Enhancement Advice (Continued)

#	Resolution
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10Gbps) or moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1Gbps are not reset to 100Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity issues might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TSO-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Storage Performance

Use the vSphere Client datastore performance charts to monitor datastore usage. Use the guidelines below to identify and correct problems with datastore performance.

NOTE The datastore charts are available only in the overview performance charts.

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. You can provision more space to the datastore if possible, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming a lot of datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information on consolidating the datacenter, see the *vSphere Client Help*.

Monitoring Host Health Status 10

You can use the vSphere Client to monitor the state of host hardware components, such as CPU processors, memory, fans, and other components.

The host health monitoring tool allows you to monitor the health of a variety of host hardware components including:

- CPU processors
- Memory
- Fans
- Temperature
- Voltage
- Power
- Network
- Battery
- Storage
- Cable/Interconnect
- Software components
- Watchdog
- Other

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware.

You can monitor a host's health status either by connecting the vSphere Client directly to a host, or by connecting to a vCenter Server system. You can also set alarms to trigger when the host health status changes.

This chapter includes the following topics:

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.

When you are connected to a host through vCenter Server, you must use the **Hardware Status** tab to monitor the host health.

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.

Monitor Health Status When Connected to vCenter Server

When you connect the vSphere Client to vCenter Server, you can view the health status from the **Hardware Status** tab.

When you are connected to a host through vCenter Server, you must use the **Hardware Status** tab to monitor the host health.

Prerequisites

Ensure that the vCenter Hardware Status plug-in is enabled.

Procedure

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

2 Select the host in the inventory and click the **Hardware Status** tab.

3 From the **View** drop-down menu, select the type of information to view.

Option	Description
Sensors	Displays all sensors arranged in a tree view. If the status is blank, the health monitoring service cannot determine the status of the component. ■ Click **Show all sensors** to expand the tree view to show all sensors under each group. ■ Click **Show all details** to expand the tree view to show descriptive details for every sensor. ■ Click **Hide all** to collapse the tree view to show only the sensor groups.
Alerts and warnings	Displays only alerts and warnings.
System event log	Displays the system event log. Click **Reset event log** to clear the event log.

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.

Procedure

1 On the host **Configuration** tab, click **Health Status**.

2 Click **Reset Sensors**.

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.

Prerequisites

Ensure that the vCenter Hardware Status plug-in is enabled.

Procedure

1 Log in to a vCenter Server system using the vSphere Client, and display the **Hosts and Clusters** view in the inventory.

2 Select the host in the inventory and click the **Hardware Status** tab.

3 Click **Reset sensors**.

Troubleshoot the Hardware Health Service

The Hardware Health service is a vCenter Server extension that uses an Internet Explorer Web browser control to display information about host hardware health. Use the information in this topic to troubleshoot problems with Hardware Health.

Procedure

◆ Take the appropriate action based on the observed problem.

Problem	Action
The Hardware Status tab is not visible in the vSphere Client.	Select **Plug-ins > Plug-in Manager** and verify that the Hardware Status plug-in is enabled.
The Hardware Status tab displays the following error message: `the remote name could not be resolved` *`SERVER_NAME`* where *`SERVER_NAME`* is the domain name of the vCenter Server system.	This error appears when the client system is unable to resolve the domain name of the vCenter Server system. Either fix the domain name resolution problem, or edit the file `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions\cim-ui\extensions.xml` on the vCenter Server system and replace the vCenter Server domain name with its IP address.
The Hardware Status tab displays a security alert.	Your Internet Explorer security settings are set too high. To change the security settings: a Launch Internet Explorer. b Select **Tools > Internet Options**. c Click the **Security** tab. d Select the **Local intranet** Web content zone. e Click **Custom Level**. f Underneath **Allow scripting of Internet Explorer Web browser control**, select **Enable**. g Click **OK** to close the Security Settings dialog box, and click **OK** to close the Internet Options dialog box.

11 SNMP and vSphere

Simple Network Management Protocol (SNMP) allows management programs to monitor and control a variety of networked devices.

Managed systems run SNMP agents, which can provide information to a management program in at least one of the following ways:

- In response to a `GET` operation, which is a specific request for information from the management system.
- By sending a trap, which is an alert sent by the SNMP agent to notify the management system of a particular event or condition.

Management Information Base (MIB) files define the information that can be provided by managed devices. The MIB files contain object identifiers (OIDs) and variables arranged in a hierarchy.

vCenter Server and ESX/ESXi have SNMP agents. The agent provided with each product has differing capabilities.

This chapter includes the following topics:

Using SNMP Traps with vCenter Server

The SNMP agent included with vCenter Server can be used to send traps when the vCenter Server system is started and when an alarm is triggered on vCenter Server. The vCenter Server SNMP agent functions only as a trap emitter, and does not support other SNMP operations, such as `GET`.

The traps sent by vCenter Server are typically sent to other management programs. You must configure your management server to interpret the SNMP traps sent by vCenter Server.

To use the vCenter Server SNMP traps, configure the SNMP settings on vCenter Server and configure your management client software to accept the traps from vCenter Server.

The traps sent by vCenter Server are defined in `VMWARE-VC-EVENT-MIB.mib`. See "VMWARE-VC-EVENT-MIB," on page 143.

Configure SNMP Settings for vCenter Server

To use SNMP with vCenter Server, you must configure SNMP settings using the vSphere Client.

Prerequisites

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 connected 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 "Configure SNMP Management Client Software," on page 135.

Configure SNMP for ESX/ESXi

ESX/ESXi includes an SNMP agent embedded in hostd that can both send traps and receive polling requests such as `GET` requests. This agent is referred to as the embedded SNMP agent.

Versions of ESX prior to ESX 4.0 included a Net-SNMP-based agent. You can continue to use this Net-SNMP-based agent in ESX 4.0 with MIBs supplied by your hardware vendor and other third-party management applications. However, to use the VMware MIB files, you must use the embedded SNMP agent.

By default, the embedded SNMP agent is disabled. To enable it, you must configure it using the vSphere CLI command `vicfg-snmp`. For a complete reference to `vicfg-snmp` options, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Prerequisites

SNMP configuration for ESX/ESXi requires the vSphere CLI. For information on installing and using the vSphere CLI, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Procedure

1 Configure SNMP Communities on page 133

Before you enable the ESX/ESXi embedded SNMP agent, you must configure at least one community for the agent.

2 Configure the SNMP Agent to Send Traps on page 133

You can use the ESX/ESX embedded SNMP agent to send virtual machine and environmental traps to management systems. To configure the agent to send traps, you must specify a target address and community.

3 Configure the SNMP Agent for Polling on page 134

If you configure the ESX/ESXi embedded SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET` requests.

4 Configure SNMP Management Client Software on page 135

After you have configured a vCenter Server system or an ESX/ESXi host to send traps, you must configure your management client software to receive and interpret those traps.

Configure SNMP Communities

Before you enable the ESX/ESXi embedded SNMP agent, you must configure at least one community for the agent.

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

Prerequisites

SNMP configuration for ESX/ESXi requires the vSphere CLI. For information on installing and using the vSphere CLI, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Procedure

- From the vSphere CLI, type
  `vicfg-snmp.pl --server hostname --username username --password password -c com1`.

  Replace *com1* with the community name you wish to set. Each time you specify a community with this command, the settings you specify overwrite the previous configuration. To specify multiple communities, separate the community names with a comma.

  For example, to set the communities public and internal on the host host.example.com, you might type **`vicfg-snmp.pl --server host.example.com --username user --password password -c public, internal`**.

Configure the SNMP Agent to Send Traps

You can use the ESX/ESX embedded SNMP agent to send virtual machine and environmental traps to management systems. To configure the agent to send traps, you must specify a target address and community.

To send traps with the SNMP agent, you must configure the target (receiver) address, community, and an optional port. If you do not specify a port, the SNMP agent sends traps to UDP port 162 on the target management system by default.

Prerequisites

SNMP configuration for ESX/ESXi requires the vSphere CLI. For information on installing and using the vSphere CLI, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Procedure

1 From the vSphere CLI, type
vicfg-snmp.pl --server *hostname* --username *username* --password *password* -t *target_address@port/community*.

Replace *target_address*, *port*, and *community* with the address of the target system, the port number to send the traps to, and the community name, respectively. Each time you specify a target with this command, the settings you specify overwrite all previously specified settings. To specify multiple targets, separate them with a comma.

For example, to send SNMP traps from the host host.example.com to port 162 on target.example.com using the public community, type
vicfg-snmp.pl --server host.example.com --username user --password password -t target.example.com@162/public.

2 (Optional) Enable the SNMP agent by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --enable.

3 (Optional) Send a test trap to verify that the agent is configured correctly by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --test.

The agent sends a `warmStart` trap to the configured target.

Configure the SNMP Agent for Polling

If you configure the ESX/ESXi embedded SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET` requests.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `vicfg-snmp` command to configure an alternative port. To avoid conflicting with other services, use a UDP port that is not defined in `/etc/services`.

IMPORTANT Both the embedded SNMP agent and the Net-SNMP-based agent available in the ESX service console listen on UDP port 161 by default. If you enable both of these agents for polling on an ESX host, you must change the port used by at least one of them.

Prerequisites

SNMP configuration for ESX/ESXi requires the vSphere CLI. For information on installing and using the vSphere CLI, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Procedure

1 From the vSphere CLI, type
vicfg-snmp.pl --server *hostname* --username *username* --password *password* -p *port*.

Replace *port* with the port for the embedded SNMP agent to use for listening for polling requests.

2 (Optional) If the SNMP agent is not enabled, enable it by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --enable.

Configure SNMP Management Client Software

After you have configured a vCenter Server system or an ESX/ESXi host to send traps, you must configure your management client software to receive and interpret those traps.

To configure your management client software, you must specify the communities for the managed device, configure the port settings, and load the VMware MIB files. Refer to the documentation for your management system for specific instructions for these steps.

Prerequisites

To complete this task, you must download the VMware MIB files from the VMware Web site: http://communities.vmware.com/community/developer/managementapi.

Procedure

1. In your management software, specify the vCenter Server or ESX/ESXi system as an SNMP-based managed device.
2. Set up appropriate community names in the management software.

   These must correspond to the communities set for the SNMP agent on the vCenter Server system or ESX/ESXi host.
3. (Optional) If you configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure the management client software to listen on the port you configured.
4. Load the VMware MIBs into the management software so you can view the symbolic names for the vCenter Server or ESX/ESXi variables.

   To prevent lookup errors, load the MIB files in the following order:

   a. `VMWARE-ROOT-MIB.mib`
   b. `VMWARE-TC-MIB.mib`
   c. `VMWARE-PRODUCTS-MIB.mib`
   d. `VMWARE-SYSTEM-MIB.mib`
   e. `VMWARE-ENV-MIB.mib`
   f. `VMWARE-RESOURCES-MIB.mib`
   g. `VMWARE-VMINFO-MIB.mib`
   h. `VMWARE-OBSOLETE-MIB.mib` (for use with versions of ESX/ESXi prior to 4.0)
   i. `VMWARE-AGENTCAP-MIB.mib`
   j. `VMWARE-VC-EVENT-MIB.mib`

The management software can now receive and interpret traps from vCenter Server or ESX/ESXi systems.

SNMP Diagnostics

Use SNMP tools to diagnose configuration problems.

You can use the following tools to diagnose problems with SNMP configuration:

- Type **`vicfg-snmp.pl --server`** ***`hostname`*** **`--username`** ***`username`*** **`--password`** ***`password`*** **`--test`** at the vSphere command-line interface to prompt the embedded SNMP agent to send a test `warmStart` trap.

- Type **vicfg-snmp.pl --server *hostname* --username *username* --password *password* --show** to display the current configuration of the embedded SNMP agent.
- The SNMPv2-MIB.mib file provides a number of counters to aid in debugging SNMP problems. See "SNMPv2 Diagnostic Counters," on page 146.
- The VMWARE-AGENTCAP-MIB.mib file defines the capabilities of the VMware SNMP agents by product version. Use this file to determine if the SNMP functionality that you want to use is supported.

Using SNMP with Guest Operating Systems

You can use SNMP to monitor guest operating systems or applications running in virtual machines.

The virtual machine uses its own virtual hardware devices. Do not install agents in the virtual machine that are intended to monitor physical hardware.

Procedure

- Install the SNMP agents you normally would use for that purpose in the guest operating systems. No special configuration is required on ESX.

VMware MIB Files

VMware MIB files define the information provided by ESX/ESXi hosts and vCenter Server to SNMP management software.

You can download these MIB files from http://communities.vmware.com/community/developer/forums/managementapi#SNMP-MIB.

Table 11-1 lists the MIB files provided by VMware and describes the information that each file provides.

Table 11-1. VMware MIB Files

MIB File	Description
VMWARE-ROOT-MIB.mib	Contains VMware's enterprise OID and top level OID assignments.
VMWARE-AGENTCAP-MIB.mib	Defines the capabilities of the VMware agents by product versions.
VMWARE-ENV-MIB.mib	Defines variables and trap types used to report on the state of physical hardware components of the host computer.
VMWARE-OBSOLETE-MIB.mib	Defines OIDs that have been made obsolete to maintain backward compatibility with earlier versions of ESX/ESXi. Includes variables formerly defined in the files VMWARE-TRAPS-MIB.mib and VMWARE-VMKERNEL-MIB.mib.
VMWARE-PRODUCTS-MIB.mib	Defines OIDs to uniquely identify each SNMP agent on each VMware platform by name, version, and build platform.
VMWARE-RESOURCES-MIB.mib	Defines variables used to report information on resource usage of the VMkernel, including physical memory, CPU, and disk utilization.
VMWARE-SYSTEM-MIB.mib	The VMWARE-SYSTEM-MIB.mib file is obsolete. Use the SNMPv2-MIB to obtain information from sysDescr.0 and sysObjec ID.0.
VMWARE-TC-MIB.mib	Defines common textual conventions used by VMware MIB files.
VMWARE-VC-EVENTS-MIB.mib	Defines traps sent by vCenter Server. Load this file if you use vCenter Server to send traps.
VMWARE-VMINFO-MIB.mib	Defines variables for reporting information about virtual machines, including virtual machine traps.

Table 11-2 lists MIB files included in the VMware MIB files package that are not created by VMware. These can be used with the VMware MIB files to provide additional information.

Table 11-2. Other MIB Files

MIB File	Description
IF-MIB.mib	Defines attributes related to physical NICs on the host system.
SNMPv2-CONF.mib	Defines conformance groups for MIBs.
SNMPv2-MIB.mib	Defines the SNMP version 2 MIB objects.
SNMPv2-TC.mib	Defines textual conventions for SNMP version 2.

VMWARE-ROOT-MIB

The VMWARE-ROOT-MIB.mib file defines the VMware enterprise OID and top level OID assignments.

Table 11-3 lists the identification mapping defined in VMWARE-ROOT-MIB.mib.

Table 11-3. Definition Mapping for VMWARE-ROOT-MIB.mib

Label	Identification Mapping
vmware	enterprises 6876
vmwSystem	vmware 1
vmwVirtMachines	vmware 2
vmwResources	vmware 3
vmwProductSpecific	vmware 4
vmwLdap	vmware 40
vmwTraps	vmware 50
vmwOID	vmware 60
vmwareAgentCapabilities	vmware 70
vmwExperimental	vmware 700
vmwObsolete	vmware 800

VMWARE-ENV-MIB

The VMWARE-ENV-MIB.mib defines variables and trap types used to report on the state of physical components of the host computer.

VMWARE-ENV-MIB.mib defines two traps:

- vmwEnvHardwareEvent, which is sent when an ESXi host has detected a material change in the physical condition of the hardware.
- vmwESXEnvHardwareEvent, which is sent when an ESX host has detected a material change in the physical condition of the hardware.

Table 11-4 lists the variables defined in VMWARE-ENV-MIB.mib.

Table 11-4. Variable Definitions in VMWARE-ENV-MIB

Variable	ID Mapping	Description
vmwEnv	vmwProductSpecific 20	Defines the OID root for this MIB module.
vmwEnvNumber	vmwEnv 1	Number of conceptual rows in vmwEnvTable.

Table 11-4. Variable Definitions in VMWARE-ENV-MIB (Continued)

Variable	ID Mapping	Description
vmwEnvLastChange	vmwEnv 2	The value of sysUptime when a conceptual row was last added to or deleted from vmwEnvTable.
vmwEnvTable	vmwEnv 3	This table is populated by monitoring subsystems such as IPMI.
vmwEnvEntry	vmwEnvTable 1	One entry is created in the table for each physical component reporting its status to ESX/ESXi.
vmwEnvIndex	vmwEnvEntry 1	A unique identifier for the physical component. This identifier does not persist across management restarts.
vmwSubsystemType	vmwEnvEntry 2	The type of hardware component that is reporting its environmental state.
vmwHardwareStatus	vmwEnvEntry 3	The last reported status of the component.
vmwEventDescription	vmwEnvEntry 4	A description of the last reported event for this hardware component.
vmwHardwareTime	vmwEnvEntry 5	The value of sysUptime when vmwHardwareStatus was reported.

VMWARE-OBSOLETE-MIB

The VMWARE-OBSOLETE-MIB.mib file contains all previously published managed objects that have been made obsolete. This file is provided to maintain compatibility with older versions of ESX/ESXi.

The variables defined in this file were originally defined in previous versions of the VMWARE-RESOURCES-MIB.mib and VMWARE-TRAPS-MIB.mib files. Table 11-5 lists the variables defined in VMWARE-OBSOLETE-MIB.mib.

Table 11-5. Variables Defined in VMWARE-OBSOLETE-MIB

Variable	ID Mapping	Description
Obsolete variables originally from VMWARE-RESOURCES-MIB		
vmwResources	vmware 3	
vmwCPU	vmwResources 1	Defines the root OID for the subtree of variables used to report CPU information.
vmwCpuTable	vmwCPU 2	A table of CPU usage by each virtual machine.
vmwCpuEntry	vmwCpuTable 1	An entry in cpuTable that records CPU usage for a single virtual machine.
vmwCpuVMID	vmwCpuEntry 1	The identification number allocated to the virtual machine by the VMkernel.
vmwCpuShares	vmwCpuEntry 2	The share of the CPU allocated to the virtual machine by the VMkernel.
vmwCpuUtil	vmwCpuEntry 3	Amount of time the virtual machine has been running on the CPU (in seconds).
vmwMemTable	vmwMemory 4	A table of memory usage by each virtual machine.

Table 11-5. Variables Defined in VMWARE-OBSOLETE-MIB (Continued)

Variable	ID Mapping	Description
vmwMemEntry	vmwMemTable 1	An entry in memTable that records memory usage by a single virtual machine.
vmwMemVMID	vmwMemEntry 1	The identification number allocated to the virtual machine by the VMkernel.
vmwMemShares	vmwMemEntry 2	The shares of memory allocated to the virtual machine by the VMkernel.
vmwMemConfigured	vmwMemEntry 3	The amount of memory the virtual machine was configured with (in KB).
vmwMemUtil	vmwMemEntry 4	The amount of memory currently used by the virtual machine (in KB).
vmwHBATable	vmwResources 3	A table used for reporting disk adapter and target information.
vmwHBAEntry	vmwHBATable 1	A record for a single HBA connected to the host machine.
vmwHbaIdx	vmwHBAEntry 1	Index for the HBA table.
vmwHbaName	vmwHBAEntry 2	A string describing the disk. Format: <devname#>:<tgt>:<lun>.
vmwHbaVMID	vmwHBAEntry 3	The identification number allocated to the running virtual machine by the VMkernel.
vmwDiskShares	vmwHBAEntry 4	Share of disk bandwidth allocated to this virtual machine.
vmwNumReads	vmwHBAEntry 5	Number of reads to this disk since the disk module was loaded.
vmwKbRead	vmwHBAEntry 6	Kilobytes read from this disk since the disk module was loaded.
vmwNumWrites	vmwHBAEntry 7	Number of writes to this disk since the disk module was loaded.
vmwKbWritten	vmwHBAEntry 8	Number of kilobytes written to this disk since the disk module was loaded.
vmwNetTable	vmwResources 4	A table used for reporting network adapter statistics.
vmwNetEntry	vmwNetTable 1	A record for a single network adapter on the virtual machine.
vmwNetIdx	vmwNetEntry 1	Index for the network table.
vmwNetName	vmwNetEntry 2	A string describing the network adapter.
vmwNetVMID	vmwNetEntry 3	The identification number allocated to the running virtual machine by the VMkernel.
vmwNetIfAddr	vmwNetEntry 4	The MAC address of the virtual machine's virtual network adapter.
vmwNetShares	vmwNetEntry 5	Share of network bandwidth allocate d to this virtual machine. This object has not been implemented.

Table 11-5. Variables Defined in VMWARE-OBSOLETE-MIB (Continued)

Variable	ID Mapping	Description
vmwNetPktsTx	vmwNetEntry 6	The number of packets transmitted on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCPktsTx.
vmwNetKbTx	vmwNetEntry 7	The number of kilobytes sent from this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCKbTx.
vmwNetPktsRx	vmwNetEntry 8	The number of packets received on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCPktsRx.
vmwNetKbRx	vmwNetEntry 9	The number of kilobytes received on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCKbRx
vmwNetHCPktsTx	vmwNetEntry 10	The number of packets transmitted on this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetPktsTx.
vmwNetHCKbTx	vmwNetEntry 11	The number of kilobytes sent from this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetKbTx.
vmwNetHCPktsRx	vmwNetEntry 12	The number of packets received on this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetPktsRx.
vmwNetHCKbRx	vmwNetEntry 13	The number of kilobytes received on this network adapter since the network module was loaded. This counter is the 64-bit versin of vmwNetKbRx.
Obsolete variables originally defined in VMWARE-TRAPS-MIB		
vmID	vmwTraps 101	The ID of the affected virtual machine generating the trap. If there is no virtual machine ID (for example, if the virtual machine has been powered off), the vmID is -1.
vmConfigFile	vmwTraps 102	The configuration file of the virtual machine generating the trap.
vpxdTrapType	vmwTraps 301	The trap type of the vCenter Server trap.
vpxdHostName	vmwTraps 302	The name of the affected host.
vpxdVMName	vmwTraps 303	The name of the affected virtual machine.
vpxdOldStatus	vmwTraps 304	The prior status.
vpxdNewStatus	vmwTraps 305	The new status.
vpxdObjValue	vmwTraps 306	The object value.

Table 11-6 lists the traps defined in VMWARE-OBSOLETE-MIB.mib. These traps were originally defined in VMWARE-TRAPS-MIB.mib.

Table 11-6. Traps Defined in VMWARE-OBSOLETE-MIB

Trap	Description
ESX/ESXi Traps	
vmPoweredOn	This trap is sent when a virtual machine is powered on from a suspended or powered off state.
vmPoweredOff	This trap is sent when a virtual machine is powered off.
vmHBLost	This trap is sent when a virtual machine detects a loss in guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmHBDetected	This trap is sent when a virtual machine detects or regains the guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmSuspended	This trap is sent when a virtual machine is suspended.
vCenter Server Traps	
vpxdTrap	This trap is sent when an entity status has changed.

VMWARE-PRODUCTS-MIB

The VMWARE–PRODUCTS–MIB.mib file defines OIDs to uniquely identify each SNMP agent on each VMware platform.

Table 11-7 lists identification mappings defined in VMWARE–PRODUCTS–MIB.mib.

Table 11-7. Identification Mappings for VMWARE-PRODUCTS-MIB.mib

Label	Identification Mapping
oidESX	vmwOID 1
vmwESX	vmwProductSpecific 1
vmwDVS	vmwProductSpecific 2
vmwVC	vmwProductSpecific 3
vmwServer	vmwProductSpecific 4

VMWARE-RESOURCES-MIB

The VMWARE–RESOURCES–MIB.mib file defines variables used to report information on resource usage.

Table 11-8 lists the identification mappings defined in VMWARE–RESOURCES–MIB.mib.

Table 11-8. Identification Mappings for VMWARE-RESOURCES-MIB

Variable	ID Mapping	Description
CPU Subtree		
vmwCPU	vmwResources 1	Defines the root OID for the subtree of variables used to report CPU information.
vmwNumCPUs	vmwCPU 1	The number of physical CPUs present on the system.
Memory Subtree		
vmwMemory	vmwResources 2	Defines the root OID for the subtree of variables used to report memory information.
vmwMemSize	vmwMemory 1	Amount of physical memory present on the host (in KB).

Table 11-8. Identification Mappings for VMWARE-RESOURCES-MIB (Continued)

Variable	ID Mapping	Description
vmwMemCOS	vmwMemory 2	Amount of physical memory allocated to the service console (in KB). This variable does not apply to ESXi hosts, which do not have a service console.
vmwMemAvail	vmwMemory 3	The amount of memory available to run virtual machines and to allocate to the hypervisor. It is computed by subtracting vmwMemCOS from vmwMemSize.
Storage Subtree		
vmwStorage	vmwResources 5	Defines the root OID for the subtree of variables used to report memory information.
vmwHostBusAdapterNumber	vmwStorage 1	The number of entries in the vmwHostBusAdapterTable.
vmwHostBusAdapterTable	vmwStorage 2	A table of Host Bus Adapters found in this host.
vmwHostBusAdapterEntry	vmwHostBusAdapterTable 1	An entry in the Host Bus Adapter table holding details for a particular adapter.
vmwHostBusAdapterIndex	vmwHostBusAdapterEntry 1	An arbitrary index assigned to this adapter.
vmwHbaDeviceName	vmwHostBusAdapterEntry 2	The system device name for this adapter.
vmwHbaBusNumber	vmwHostBusAdapterEntry 3	The host bus number. For unsupported adapters, returns -1.
vmwHbaStatus	vmwHostBusAdapterEntry 4	The operational status of the adapter.
vmwHbaModelName	vmwHostBusAdapterEntry 5	The model name of the adapter.
vmwHbaDriverName	vmwHostBusAdapterEntry 6	The name of the adapter driver.
vmwHbaPci	vmwHostBusAdapterEntry 7	The PCI ID of the adapter.

VMWARE-SYSTEM-MIB

The VMWARE-SYSTEM-MIB.mib file provides variables for identifying the VMware software running on a managed system by product name, version number, and build number.

Table 11-9 lists the variables defined in VMWARE-SYSTEM-MIB.mib.

Table 11-9. Variables Defined in VMWARE-SYSTEM-MIB

Variable	ID Mapping	Description
vmwProdName	vmwSystem 1	The product name.
vmwProdVersion	vmwSystem 2	The product version number, in the format *Major.Minor.Update*.
vmwProdBuild	vmwSystem 4	The product build number.

VMWARE-TC-MIB

The VMWARE-TC-MIB.mib file provides common textual conventions used by VMware MIB files.

VMWARE-TC-MIB.mib defines the following integer values for VmwSubsystemTypes:

- unknown(1)
- chassis(2)
- powerSupply(3)
- fan(4)

- cpu(5)
- memory(6)
- battery(7)
- temperatureSensor(8)
- raidController(9)
- voltage(10)

VMWARE-TC-MIB.mib defines the following integer values for VmwSubsystemStatus:

- unknown(1)
- normal(2)
- marginal(3)
- critical(4)
- failed(5)

VMWARE-VC-EVENT-MIB

The VMWARE-VC-EVENT-MIB.mib file provides definitions for traps sent by vCenter Server. These definitions were provided by VMWARE-TRAPS-MIB.mib in earlier versions of VirtualCenter Server.

Table 11-10 lists the traps defined for vCenter Server.

Table 11-10. Alarms Defined in VMWARE-VC-EVENT-MIB

Trap	ID Mapping	Description
vpxdAlarm	vmwVCNotifications 201	The vCenter Server SNMP agent sends this trap when an entity's alarm status changes.
vpxdDiagnostic	vmwVCNotifications 202	The vCenter Server SNMP agent sends this trap when vCenter Server starts or is restarted, or when a test notification is requested. vCenter Server can be configured to send this trap periodically at regular intervals.

Table 11-11 lists the variables defined for the vCenter Server traps.

Table 11-11. Variables Defined in VMWARE-VC-EVENT-MIB

Variable	ID Mapping	Description
vmwVpxdTrapType	vmwVC 301	The trap type of the vCenter Server trap.
vmwVpxdHostName	vmwVC 302	The name of the affected host.
vmwVpxdVMName	vmwVC 303	The name of the affected virtual machine.
vmwVpxdOldStatus	vmwVC 304	The prior status.
vmwVpxdNewStatus	vmwVC 305	The new status.
vmwVpxdObjValue	vmwVC 306	The object value.

VMWARE-VMINFO-MIB

The VMWARE-VMINFO-MIB.mib file defines variables and traps for reporting virtual machine information.

Table 11-12 lists the variables defined in VMWARE-VMINFO-MIB.mib.

Table 11-12. Identification Mappings for VMWARE-VMINFO-MIB

Variable	ID Mapping	Description
Virtual Machine Variables		
vmwVmTable	vmwVirtMachines 1	A table containing information on the virtual machines that have been configured on the system.
vmwVmEntry	vmwVmTable 1	The record for a single virtual machine.
vmwVmIdx	vmwVmEntry 1	An index for the virtual machine entry.
vmwVmDisplayName	vmwVmEntry 2	The display name for the virtual machine.
vmwVmConfigFile	vmwVmEntry 3	The path to the configuration file for this virtual machine.
vmwVmGuestOS	vmwVmEntry 4	The guest operating system running on the virtual machine.
vmwVmMemSize	vmwVmEntry 5	The memory (in MB) configured for this virtual machine.
vmwVmState	vmwVmEntry 6	The virtual machine power state (on or off).
vmwVmVMID	vmwVmEntry 7	An identification number assigned to running virtual machines by the VMkernel. Powered-off virtual machines to not have this ID.
vmwVmGuestState	vmwVmEntry 8	The state of the guest operating system (on or off).
vmwVmCpus	vmwVmEntry 9	The number of virtual CPUs assigned to this virtual machine.
Virtual Machine HBA Variables		
vmwVmHbaTable	vmwVirtMachines 2	A table of HBAs visible to a virtual machine.
vmwVmHbaEntry	vmwVmHbaTable 1	Record for a single HBA.
vmwHbaVmIdx	vmwVmHbaEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwVmHbaIdx	vmwVmHbaEntry 2	Uniquely identifies a given HBA in this VM. May change across system reboots.
vmwHbaNum	vmwVmHbaEntry 3	The name of the HBA as it appears in the virtual machine settings.
vmwHbaVirtDev	vmwVmHbaEntry 4	The HBA hardware being emulated to the guest operating system.
vmwHbaTgtTable	vmwVirtMachines 3	The table of all virtual disks configure for virtual machines in vmwVmTable.
vmwHbaTgtEntry	vmwHbaTgtTable 1	A record for a specific storage disk. May change across reboots.
vmwHbaTgtVmIdx	vmwHbaTgtEntry 1	A number corresponding to the virtual machine's index (vmwVmIdx) in the vmwVmTable.
vmwHbaTgtIdx	vmwHbaTgtEntry 2	This value identifies a particular disk.
vmwHbaTgtNum	vmwHbaTgtEntry 3	Identifies the disk as seen from the host bus controller.
Virtual Machine Network Variables		
vmwVmNetTable	vmwVirtMachines 4	A table of network adapters for all virtual machines in vmwVmTable.
vmwVmNetEntry	vmwVmNetTable 1	Identifies a unique network adapter in this table.
vmwVmNetVmIdx	vmwVmNetEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.

Table 11-12. Identification Mappings for VMWARE-VMINFO-MIB (Continued)

Variable	ID Mapping	Description
vmwVmNetIdx	vmwVmNetEntry 2	Identifies a unique network adapter in this table. May change across sytem reboots.
vmwVmNetNum	vmwVmNetEntry 3	The name of the network adapter as it appears in the virtual machine settings.
vmwVmNetName	vmwVmNetEntry 4	Identifies what the network adapter is connected to.
vmwVmNetConnType	vmwVmNetEntry 5	Obsolete. Do not use.
vmwVmNetConnected	vmwVmNetEntry 6	Reports true if the ethernet virtual device is connected to the virtual machine.
vmwVmMAC	vmwVmNetEntry 7	Reports the configured virtual hardware MAC address. If VMware Tools is not running, the value is zero or empty.
Virtual Floppy Device Variables		
vmwFloppyTable	vmwVirtMachines 5	A table of floppy drives for all virtual machines in vmwVmTable.
vmwFloppyEntry	vmwFloppyTable 1	Identifies a single floppy device. May change across system reboots.
vmwFdVmIdx	vmwFloppyEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwFdIdx	vmwFloppyEntry 2	Identifies a specific virtual floppy device.
vmwFdName	vmwFloppyEntry 3	The file or device that this virtual floppy device is connected to.
vmwFdConnected	vmwFloppyEntry 4	Reports true if the floppy device is connected.
Virtual DVD or CD-ROM Variables		
vmwCdromTable	vmwVirtMachines 6	A table of DVD or CD-ROM drives for all virtual machines in vmwVmTable.
vmwCdromEntry	vmwCdromTable 1	Identifies a specific CD-ROM or DVD drive. May change across system reboots.
vmwCdVmIdx	vmwCdromEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwCdromIdx	vmwCdromEntry 2	Identifies the specific DVD or CD-ROM drive.
vmwCdromName	vmwCdromEntry 3	The file or device that the virtual DVD or CD-ROM drive has been configured to use.
vmwCdromConnected	vmwCdromEntry 4	Reports true the CD-ROM device is connected.
Virtual Machine Trap Variables		
vmwVmID	vmwTraps 101	Holds the same value as vmwVmVMID of the affected virtual machine generating the trap, to allow polling of the affected virtual machine in vmwVmTable.
vmwVmConfigFilePath	vmwTraps 102	The configuration file of the virtual machine generating the trap.

Table 11-13 lists the traps defined in VMWARE-VMINFO-MIB.mib. These traps were formely defined in VMWARE-TRAPS-MIB.mib.

Table 11-13. Traps Defined in VMWARE-VMINFO-MIB

Trap	ID Mapping	Description
vmwVmPoweredOn	vmwVmNotifications 1	This trap is sent when a virtual machine is powered on from a suspended or powered off state.
vmwVmPoweredOff	vmwVmNotifications 2	This trap is sent when a virtual machine is powered off.
vmwVmHBLost	vmwVmNotifications 3	This trap is sent when a virtual machine detects a loss in guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmwVmHBDetected	vmwVmNotifications 4	This trap is sent when a virtual machine detects or regains the guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmwVmSuspended	vmwVmNotifications 5	This trap is sent when a virtual machine is suspended.

SNMPv2 Diagnostic Counters

The SNMPv2-MIB.mib file provides a number of counters to aid in debugging SNMP problems.

Table 11-14 lists some of these diagnostic counters.

Table 11-14. Diagnostic Counters from SNMPv2-MIB

Variable	ID Mapping	Description
snmpInPkts	snmp 1	The total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	snmp 3	The total number of SNMP messages that were delivered to the SNMP entity and were for an unsupported SNMP version.
snmpInBadCommunityNames	snmp 4	The total number of community-based SNMP messages delivered to the SNMP entity that used an invalid SNMP community name.
snmpInBadCommunityUses	snmp 5	The total number of community-based SNMP messages delivered to the SNMP entity that represented an SNMP operation that was not allowed for the community named in the message.
snmpInASNParseErrs	snmp 6	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpEnableAuthenTraps	snmp 30	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information. It therefore provides a means of disabling all authenticationFailure traps.

Table 11-14. Diagnostic Counters from SNMPv2-MIB (Continued)

Variable	ID Mapping	Description
snmpSilentDrops	snmp 31	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate Response Class PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	snmp 32	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in a manner other than a time-out such that no Response Class PDU could be returned.

12 Monitoring Storage Resources

If you use vCenter Server to manage your ESX/ESXi hosts, you can review information on storage usage and visually map relationships between all storage entities available in vCenter Server.

In the vSphere Client, for any inventory object except networking, the storage usage data appears in the **Storage Views** tab. To view this tab, you must have the vCenter Storage Monitoring plug-in, which is generally installed and enabled by default.

You can display storage information as reports or storage topology maps.

Reports — Reports display relationship tables that provide insight about how an inventory object is associated with storage entities. They also offer summarized storage usage data for the object's virtual and physical storage resources. Use the **Reports** view to analyze storage space utilization and availability, multipathing status, and other storage properties of the selected object and items related to it.

Maps — Maps display storage topology maps that visually represent relationships between the selected object and its associated virtual and physical storage entities.

For more information about virtual and physical storage resources and how virtual machines access storage, see *ESX Configuration Guide* or *ESXi Configuration Guide*.

This chapter includes the following topics:

Working with Storage Reports

Reports help you monitor storage information.

You can display and review statistics for different categories depending on the inventory object. For example, if the inventory object is a datastore, you can display information for virtual machines that reside on the datastore, hosts that have access to the datastore, the LUNs on which the datastore is deployed, and so on.

When you display the report tables, the default column headings depend on the inventory object you select. You can customize the tables by adding or removing columns. Reports are updated every 30 minutes. You can manually update the reports by clicking **Update**.

You can search for information that you need by filtering report tables based on storage attributes and keywords.

Display Storage Reports

You display storage reports to review storage information for any inventory object except networking. For example, if the inventory object is a virtual machine, you can review datastores and LUNs that the virtual machine uses, status of paths to the LUNs, adapters that the host uses to access the LUNs, and so on.

Procedure

1 Display the object, for which you want to view reports, in the inventory.

For example, display virtual machines to review storage information for a specific virtual machine.

2 Select the object and click **Storage Views > Reports**.

3 To show information for a specific category, click **Show all [Category of Items]** and select the appropriate category from the list.

For example, to see all datastores that the virtual machine is using, select **Show all Datastores**.

4 To see the description of each column, move the cursor over the column heading.

Export Storage Reports

You can export storage usage data for an object in various formats, including XML, HTML, or Microsoft Excel.

Perform the following task in the vSphere Client.

Procedure

1 Display the object in the inventory.

2 Select the object and click **Storage Views > Reports**.

3 To display information for a specific category, click **Show all [Category of Items]**and select the appropriate category from the list.

4 Right-click below the table and select **Export List**.

5 Specify a file name, type, and location.

6 Click **Save**.

Filter Storage Reports

To search for specific information, you can filter reports based on any number of storage attributes you select and keywords you enter in the search field.

Procedure

1 In the inventory, display the object for which to filter the reports.

2 Select the object and click **Storage Views > Reports**.

3 To display information for a specific category, click **Show all [Category of Items]**and select the appropriate category from the list.

4 Click the search field arrow and select the attributes to include in the search.

5 Type a keyword into the box and press **Enter**.

The table is updated based on your search criteria. For example, if you are reviewing reports for datastores in a datacenter, you can display information for only those datastores that have NFS format by selecting the **File System Type** attribute and entering NFS as a key word. Filtering is persistent for the user session.

Customize Storage Reports

You display storage reports in the vSphere Client. When you display the reports tables, the default column headings depend on the inventory object you select. You can customize the tables by adding or removing columns.

Procedure

1 Display the object in the inventory for which you want to customize reports.

2 Select the object and click **Storage Views > Reports**.

3 To display information for a specific category, click **Show all [Category of Items]**and select the appropriate category from the list.

4 To add a column, right-click any column heading and select an item to display from the list.

5 To hide a column, right-click the column heading and deselect it in the list.

Working with Storage Maps

Storage maps help you visually represent and understand the relationships between an inventory object and all virtual and physical storage resources available for this object. Map views are object-centric and display only items relevant to the specific object.

Map views are updated every 30 minutes. You can manually update the maps by clicking the **Update** link.

You can customize a map view by selecting or deselecting options in the Show area, or by hiding specific items or changing their position on the map.

You can reposition the map by dragging it, and zoom in or out of the map or its particular section.

Display Storage Maps

For any inventory object except networking, you can display storage maps that graphically represent the relationships between the object, for example, a virtual machine, and all resources, such as datastores, LUNs, hosts, and so on, available for this object.

Procedure

1 Display the object in the inventory.

2 Select the object and click **Storage Views > Maps**.

Export Storage Maps

You can export maps to various graphic files, including JPEG, TIFF, and GIF.

Procedure

1 Display a storage map.

2 Right-click the map and select **Export Map** from the menu.

3 Type a file name, type, and location.

4 Click **Save**.

The image file is saved to the format and directory you specified.

Hide Items on Storage Maps

You can hide any number of items in a storage map.

Procedure

1 Display a storage map.

2 Right-click the item you want to hide and select **Hide Node** from the menu.

Move Items on Storage Maps

You might need to move individual items on the storage map to make the map visually more clear.

Procedure

1 Display a storage map.

2 Click the item you want to move and drag it to the new location.

Working with Alarms 13

Alarms are notifications that occur in response to selected events, conditions, and states that occur with objects in the inventory. You use the vSphere Client to create and modify alarms.

The vCenter Server system is configured with a set of predefined alarms that monitor clusters, hosts, datacenters, datastores, networks, and virtual machines. it is also configured with alarms that monitor vCenter Server licensing.

Each predefined alarm monitors a specific object and applies to all objects of that type. For example, by default, the Host CPU Usage alarm is set automatically on each host in the inventory and triggers automatically when any host's CPU usage reaches the defined CPU value.

If the predefined vCenter Server alarms do not account for the condition, state, or event you need to monitor, you can define custom alarms.

When you set an alarm on a parent object, such as a vCenter Server, a datacenter, or a cluster, all applicable child objects inherit the alarm. You can also set an alarm on a folder to propagate the same alarm to all objects contained in that folder. You cannot change or override an alarm that is set on a child object from its parent object. You must change the alarm on the child object itself.

Alarms are composed of a trigger and an action.

Trigger

A set of conditions that must be met for an alarm warning and alert to occur. Most triggers consist of a condition value and a length of time that value is true. For example, the virtual machine memory alarm triggers a warning when memory usage is over 75% for one hour and over 90% for five minutes.

VMware uses colors to denote alarm severity:

- Normal – green
- Warning – yellow
- Alert – red

You can set alarms to trigger when the state changes from green to yellow, yellow to red, red to yellow, and yellow to green. Triggers are defined for the default VMware alarms. You can change the trigger conditions (thresholds, warning values, and alert values) for the default alarms.

Action The operation that occurs in response to the trigger. For example, you can have an email notification sent to one or more administrators when an alarm is triggered. The default vCenter Server alarms are not preconfigured with actions. You must manually set what action occurs when the triggering event, condition, or state occurs.

NOTE Some alarms contain triggers that are not supported in the vSphere Client and cannot be changed. However, you can still configure the alarm actions, enable or disable the alarm, and change the alarm name. If your environment requires changes to these alarm triggers, create custom alarms by using the vSphere Client or the VMware vSphere APIs.

This chapter includes the following topics:

Alarm Triggers

You configure alarm triggers to generate warnings and alerts when the specified criteria is met. Alarms have two types of triggers: condition or state triggers, and event triggers.

Condition or State Triggers Monitor the current condition or state of virtual machines, hosts, and datastores. This includes power states, connection states, and performance metrics, such as CPU and disk usage. To set alarms on other objects in the inventory, including datacenters, clusters, resource pools, and networking objects, use event triggers.

NOTE You can set a condition or state alarm at the datacenter level that monitors all virtual machines, hosts, or datastores in the datacenter.

Event Triggers Monitors events that occur in response to operations occurring with any managed object in the inventory, the vCenter Server system, or the license server. For example, an event is recorded each time a virtual machine is cloned, created, deleted, deployed, and migrated.

Condition and State Triggers

Use condition triggers and state triggers to set alarms on performance metrics, power states, and connection states for virtual machines, hosts, and datastores. To set alarms on other objects in the inventory, you must use event triggers.

Condition and state triggers use one of the following operator sets to monitor an object:

- **Is equal to** and **Is not equal to**

- **Is above** and **Is below**

To define a condition or state trigger, you choose the appropriate operator set and enter the values for the warning and alert status. You can use any number of triggers for an alarm. When you use more than one trigger, you choose whether to trigger the alarm when any conditions are satisfied or when all conditions are satisfied. For example, you can create a host alarm that has two condition triggers, one for CPU usage and one for memory usage:

Table 13-1. Example - Host Alarm with Condition Triggers

		Warning		Alert	
Trigger	**Condition**	**Operator**	**Value**	**Operator**	**Value**
1	CPU usage	Is above	75%	Is above	90%
2	Memory usage	Is above	75%	Is above	90%

If you trigger the alarm when all conditions are satisfied, the alarm will trigger the warning only when both CPU usage and memory usage values are above 75%. Likewise, it will trigger the alert only when both CPU usage and memory usage are above 90%.

NOTE Unexpected results might occur when you have an alarm with multiple triggers with opposing warning and alert conditions, and you set the alarm to trigger when all conditions are satisfied. For example, an alarm has two triggers that set warnings and alerts for the virtual machine power state.

Table 13-2. Example – Opposing Warning and Alert Conditions

Trigger	**Warning**	**Alert**
1	Powered Off	Powered On
2	Powered On	Powered Off

If you choose to trigger the alarm when all conditions are satisfied, the alarm triggers a warning. This is because the vServer System uses the AndAlarmExpression operator to validate the condition statuses for each trigger. When they are all satisfied, the first condition is satisfied, and therefore is used: Warning & Alert = warning.

Condition and State Trigger Components

Condition and State triggers are comprised of a trigger type, a triggering condition and length, and warning and alert values.

Table 13-3 describes each component of Condition and State triggers.

Table 13-3. Condition and State Trigger Components

Trigger Component	**Description**
Trigger type	The condition or state to monitor, for example, **VM CPU Usage (%)**.
Condition	The qualifier used to set the threshold for the trigger, for example, **Is Above** and **Is Below**.
Warning	The value that must be reached for the alarm to transition from a normal state to a warning state, and to trigger the alarm.
Condition Length	For condition triggers, after the warning condition is reached, the amount of time the warning condition stays true in order for the warning to trigger. State triggers do not have condition lengths. As soon as the state condition occurs, the warning is triggered.

Table 13-3. Condition and State Trigger Components (Continued)

Trigger Component	Description
Alert	The value that must be reached for the alarm to transition from the warning state to an alert state and to trigger the alarm.
Condition Length	For condition triggers, after the alert value is reached, the amount of time the alert condition stays true in order for the alarm to trigger. State triggers do not have condition lengths. As soon as the state condition occurs, the alert is triggered.

For condition triggers to generate a warning or an alert, the value you set must be reached and for the specified condition length. For example, you can configure a condition trigger to generate a warning and an alert under the following conditions:

- A virtual machine's CPU usage must be above 75% for more than 10 minutes to generate a warning.
- A virtual machine's CPU usage must be above 95% for more than 5 minutes to generate a warning.

The 10 minute and 5 minute time conditions in this example help distinguish an erratic condition from a true scenario. You set time requisites to ensure that the metric conditions are valid and not caused by incidental spikes.

Triggered alarms reset when the triggering condition or state is no longer true. For example, if you have an alarm defined to trigger a warning when host CPU is above 75%, the condition will reset to normal when the value falls below the 75% and the warning alarm will no longer be triggered. The threshold condition is dependent on any tolerance range you set for the threshold.

Virtual Machine Condition and State Triggers

VMware provides default triggers that you can use to define alarms on virtual machines when they undergo certain conditions and states.

Table 13-4 lists the Condition and State triggers you can set on virtual machines.

Table 13-4. Virtual Machine Condition and State Alarm Triggers

Trigger Type	Trigger Name	Description
Condition	CPU Ready Time (ms)	The amount of time the virtual machine was ready during the collection interval, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads.
Condition	CPU Usage (%)	Amount of virtual CPU (MHz) used by the virtual machine. CPU limits are ignored in the calculation. The calculation is: VM CPU Usage (%) = VM CPU [MHz] / (# of vCPUs x clock rate of the physical CPU [MHz]) x 100
Condition	Disk Aborts	Number of SCSI commands that were not completed on each physical disk of the virtual machine.
Condition	Disk Resets	Number of SCSI-bus reset commands issued on each physical disk of the virtual machine.
Condition	Disk Usage (KBps)	Sum of the data read and written across all disk instances on the virtual machine.
Condition	Fault Tolerance Secondary VM Latency Status Changed	Amount of wallclock time that the virtual CPU of the secondary virtual machine is behind the virtual CPU of the primary virtual machine. ■ Low – 0-2 seconds ■ Moderate – 2-6 seconds ■ High – More than 6 seconds

Table 13-4. Virtual Machine Condition and State Alarm Triggers (Continued)

Trigger Type	Trigger Name	Description
State	Heartbeat	Current status of the guest operating system heartbeat: ■ Gray – VMware Tools are not installed or not running. ■ Red – No heartbeat. Guest operating system may have stopped responding. ■ Yellow – Intermittent heartbeat. A Yellow status may be caused by heavy guest OS usage. ■ Green – Guest operating system is responding normally.
Condition	Memory Usage (%)	Amount of configured RAM (MB) used by the virtual machine. The calculation is: VM Memory Usage (%) = Active Memory [MB] / configured RAM of VM [MB] x 100
Condition	Network Usage (Kbps)	Sum of data transmitted and received across all virtual NIC instances on the virtual machine.
Condition	Snapshot Size (GB)	Aggregate size (KB) of all snapshots taken for the current virtual machine.
State	State	Current state of the virtual machine: ■ Powered On – The virtual machine is powered on. ■ Powered Off – The virtual machine is powered off. ■ Suspended – The virtual machine is suspended.
Condition	Total Disk Latency (ms)	Average amount of time taken to process a SCSI command issued by the Guest OS to the virtual machine. The calculation is: Total Disk Latency = kernelLatency + deviceLatency ■ Low – 0-2 seconds ■ Moderate – 2-6 seconds ■ High – More than 6 seconds
Condition	Total Size on Disk (GB)	Aggregate amount of disk space occupied by all virtual machines on the host.

Host Condition and State Triggers

VMware provides preconfigured alarms that trigger when hosts undergo certain conditions and states.

Table 13-5 lists the default Condition and State triggers you can set on hosts.

Table 13-5. Host Condition and State Triggers

Trigger Name	Description	Trigger Type
Connection State	Current connection state of the host: ■ Connected – The host is connected to the server. For ESX/ESXi hosts, this is always the state. ■ Disconnected – A user has explicitly shut down the host. In this state, vCenter Server does not expect to receive heartbeats from the host. The next time a heartbeat is received, the host is returned to a connected state and an event is logged. ■ Not Responding – vCenter Server is not receiving heartbeat messages from the host. After the heartbeat messages are received again, the state automatically changes to Connected. This state is often used to trigger an alarm on the host.	State
Console SwapIn Rate (KBps)	Rate at which the service console kernel is swapping in memory. The Console Swapin Rate indicates memory pressure in the service console. A high value is generally a precursor to timeout operations. To fix the problem, consider adding more memory or ending the memory-intensive task.	Condition

Table 13-5. Host Condition and State Triggers (Continued)

Trigger Name	Description	Trigger Type
Console SwapOut Rate (KBps)	Rate at which the service console kernel is swapping out memory. The Console Swapout Rate indicates memory pressure in the service console. A high value is generally a precursor to timeout operations. To fix the problem, consider adding more memory or ending the memory-intensive task.	Condition
CPU Usage (%)	Amount of physical CPU (MHz) used by the ESX/ESXi host. The calculation is: Host CPU Usage (%) = CPU usage [MHz] / (# of physical CPUs x clock rate [MHz]) x 100	Condition
Disk Usage (KBps)	Sum of the data read from and written to all disk instances on the host.	Condition
Memory Usage (%)	Amount of physical RAM (MB) consumed by the ESX/ESXi host. The calculation is: Host Memory Usage (%) = Consumed Memory [MB] / physical RAM of server [MB] x 100	Condition
Network Usage (kbps)	Sum of data transmitted and received for all the NIC instances of the host.	Condition
Power State	Current power state of the host: ■ Powered On – The host is powered on. ■ Powered Off – The host is powered off. ■ Suspended – The host is suspended.	State
Swap Pages Write (KBps)	Rate at which host memory is swapped out to the disk.	Condition

Datastore Condition and State Triggers

VMware provides preconfigured alarms that trigger when datastores undergo certain conditions and states.

Table 13-6 lists the default Condition and State triggers you can set on datastores.

Table 13-6. Datastore Condition and State Triggers

Trigger Type	Trigger Name	Description
Condition	Datastore Disk Overallocation (%)	Amount of overallocated disk space in the datastore.
Condition	Datastore Disk Usage (%)	Amount of disk space (KB) used by the datastore. NOTE This alarm controls the **Status** value for datastores in vSphere Client. If you disable this alarm, the datastore status will be displayed as **Unknown**.
State	Datastore State to All Hosts	■ Connected to all hosts – The datastore is connected to at least one host. ■ Disconnected from all hosts – The datastore is disconnected from at least one host.

Event Triggers

Event triggers monitor events that occur in response to actions related to managed objects, the vCenter Server system, and the License Server.

Event triggers use arguments, operators, and values to monitor operations that occur in the vServer System. Because the occurrance of the event gives you information about the operation occurring in your environment, you usually will not need to configure arguments for them. However, some events are general and configuration might be required to set the alarm on the desired information. For example, the Hardware Health Changed event occurs for a variety of different subsystems on a host.The preconfigured datacenter alarm Host Hardware Fan Health uses the Hardware Health Changed event with the following two arguments to set a warning condition when a fan is not operating:

Table 13-7. Example – Event Arguments, Operators, and Values

Argument	Operator	Value
group	equal to	Fan
newState	equal to	Yellow

NOTE Due to the large number of events tracked by vCenter Server, the event table for each object does not contain definitive lists of events. Instead, it provides a subset of the events available for alarm triggers.

Event Trigger Components

Event triggers are composed of a trigger type, a trigger status, and triggering conditions.

Table 13-8 describes the components of event alarm triggers.

Table 13-8. Event Trigger Components

Trigger Component	Description
Trigger type	Event to monitor. Events can be generated by a user action or the system, for example, Account Password Change and Alarm Email Sent.
Status	The value that must be met for the alarm to trigger: ■ Normal ■ Warning ■ Alert
Conditions	Specifications that define the trigger. Event conditions include the following components: ■ Argument – The event attribute to monitor. ■ Operator – The qualifier used to set the trigger value, for example **Starts with** and **Doesn't start with**. ■ Value – The value that must be met to trigger the event. Conditions are not configurable for all events.

For example, you have a subset of hosts in the same datacenter named with the identifying prefix, `QA_`. To trigger an alarm when any of these hosts lose network connectivity, create an alarm on the datacenter to monitor the event `Lost Network Connectivity`. The trigger conditions are:

- Argument — `host.name`
- Operator — `Starts with`
- Value – `QA_`

When storage connectivity is lost on a host named QA_Host1, the event triggers.

Event triggers do not rely on thresholds or durations. They use the arguments, operators, and values to identify the triggering condition. When the triggering conditions are no longer true, a triggered alarm resets automatically, and no longer triggers.

Virtual Machine Event Triggers

VMware provides preconfigured alarms that trigger when events occur on virtual machines.

Table 13-9 lists events you can use to trigger alarms on virtual machines.

Table 13-9. Virtual Machine Event Triggers

Event Category	Available Events
Customization	Customization started, Customization succeeded, Cannot complete Sysprep, Unknown error.
Deployment	VM created, VM auto renamed, VM being closed, VM being creating, VM deploying, VM emigrating, VM hot migrating, VM migrating, VM reconfigured, VM registered, VM removed, VM renamed, VM relocating, VM upgrading. Cannot complete clone, Cannot migrate, Cannot relocate, Cannot upgrade.
DRS	DRS VM migrated, VM powered on, No maintenance mode DRS recommendation.
Fault tolerance	Secondary VM added, Secondary VM disabled, Secondary VM enabled, Secondary VM started. vCenter cannot start secondary VM, vCenter cannot update secondary VM configuration, vCenter disabled fault tolerance. Fault tolerance state changed, Fault tolerance turned off, Fault tolerance VM deleted. No compatible host for secondary VM. Reached maximum Secondary VM (with FT turned On) restart count.
General messages and information	VM error, VM error message, VM information, VM information message, VM warning, VM warning message, VM migration error, VM migration warning, VM configuration missing.
HA	HA enabled VM reset, No HA enabled port groups, Cannot reset HA enabled VM, VM HA updated error, Insufficient failover resources.
Naming and IDs	UUID: Assigned, Changed, Conflict. Assign a new instance, Instance changed, Instance conflict. MAC: Assigned, Changed, Conflict. VM static MAC conflict. WWN: Assigned, Changed, Conflict.
Power and connection states	VM connected, VM disconnected, VM discovered, VM powered off, VM powered on, VM starting, VM stopping, VM suspended, VM restarted on alternate host, VM resuming. Guest reboot, guest shutdown, guest standby. Cannot power off, Cannot power on, Cannot reboot guest OS, Cannot reset, Cannot shut down the guest OS, Cannot standby guest OS, Cannot suspend. Remote console connected, Remote console disconnected.
Record, Replay	Start a recording session, Start a replay session.
Resource Pool	Resource pool moved, Resource pool relocated.

Host Event Triggers

VMware provides preconfigured alarms that trigger when events occur on hosts.

Table 13-10 lists events you can use to trigger alarms on hosts.

Table 13-10. Host Event Triggers

Event Category	Available Events
Accounts	Account created, Account removed, Account updated.
Access and security	Administrator access disabled, Administrator access enabled. Administrator password not changed. VIM account password changed. License expired, No license.
Connection and mode	Host connected, Host disconnected. Host entered maintenance mode, Host exited maintenance mode, Host entering standby mode, Host exiting standby mode. Cannot connect host, cannot get host short name, Host already managed, Incorrect Ccagent, Incorrect user name, Incompatible version, Ccagent upgrade, Network error, No access. Connection lost, Cannot reconnect host, Host connection failure, Network connectivity lost, Network uplink redundancy degraded, Network uplink redundancy lost, Cannot connect to storage.
DRS	DRS entering standby mode, DRS exited standby mode, DRS exiting standby mode. Cannot complete DRS resource configuration, Resource configuration synchronized.
vDS	Distributed Virtual Switch joined the port group, Distributed Virtual Switch left the port group, Distributed Virtual Switch does not exist in vCenter or does not contain this host.
General error information	Host error, Host information, Host warning.
HA	Host HA agent disabled, HA agent enabled, Disabling HA, Enabling HA agent, HA agent error, HA agent configured. Host has extra HA networks, Host has no available HA networks, Host is missing HA networks, No redundant management network for host, No HA enabled port groups.
Hardware health	Hardware health changed
Inventory	Host added, Host not in cluster. No datastores configured.
IP address	Host IP changed, IP inconsistent, IP to short name not completed, Cannot get short host name, Short name to IP not completed, Duplicate IP detected.
vCenter Agent	Cannot complete vCenter Agent, Cannot uninstall vCenter Agent.

Datastore Event Triggers

VMware provides preconfigured alarms that trigger when events occur on datastores.

Table 13-11 lists events you can use to trigger alarms on datastores.

Table 13-11. Datastore Event Triggers

Event Category	Available Events
Datastore modification	Datastore capacity increased. Local datastore created, Datastore deleted, Datastore discovered, Datastore removed from host.
File system operations	File or directory copied to datastore, File or directory deleted from datastore, File or directory moved to datastore.
NAS	NAS datastore created.
VMFS	VMFS datastore created, VMFS datastore expanded, VMFS datastore extended.

Datacenter Event Triggers

VMware provides preconfigured alarms that trigger when events occur on datacenters.

Table 13-12 lists events you can use to set alarms on datacenters.

Table 13-12. Datacenter Event Triggers

Event Category	Available Events
Alarms	Alarm created, reconfigured, removed. Alarm email sent, email send failed. Alarm script completed, script not completed. Alarm SNMP trap sent, SNMP trap not completed. Alarm status changed.
Authentication, Permissions, and Roles	Already authenticated. Permission added, removed, updated. Profile created, removed. Role added, created, removed.
Custom Fields	Custom field definition added, removed, renamed. Custom field value changed. cannot complete customization network setup.
Customization	Customization Linux identity failed, network setup failed.
Datacenter	Datacenter created, renamed.
Datastore	Datastore renamed, datastore renamed on host.
DRS	DRS invocation not completed, DRS recovered from failure.
vDS	vNetwork Distributed Switch merged, renamed, configuration on some hosts differed from that of the vCenter Server.
HA and DRS	HA agent found, DRS invocation not completed, DRS recovered from failure.
Hosts	Host add failed, inventory full, short name inconsistent, cannot add host.
Licensing	License added, assigned, expired, insufficient, removed, unassigned. License server available, unavailable. Unlicensed virtual machines, all virtual machines licensed.
Scheduled Tasks	Scheduled task created, completed, cannot complete, email sent, email not sent, reconfigured, removed, started.
Templates	Upgrading template, template upgraded, cannot upgrade template.
User Operations	User assigned to group, removed from group, login, logout, upgrade.
Virtual Machines	VM cloned, created, relocated, upgraded.
vServer	Server license expired, session started, session stopped.

Cluster Event Triggers

VMware provides preconfigured alarms that trigger when events occur on clusters.

Table 13-13 lists events you can use to set alarms on clusters.

Table 13-13. Cluster Event Triggers

Event Category	Available Events
Cluster creation, modification, and compliance	Cluster created, Cluster deleted, Cluster overcommitted, Cluster reconfigured. Cluster status changed, Cluster compliance checked.
High Availability (HA)	HA agent unavailable, HA disabled, HA enabled, HA host failed, HA host isolated, All HA hosts isolated, Cluster overcommitted, Virtual machine heart beat failed.
DRS	DRS enabled, DRS disabled.

dvPort Group Event Triggers

VMware provides preconfigured alarms that trigger when events occur on dvPort group alarms.

Table 13-14 lists events you can use to set alarms on dvPort groups.

Table 13-14. dvPort Group Event Triggers

Event Category	Available Events
Distributed Virtual Port Group	Distributed virtual group created, Distributed virtual group deleted, Distributed virtual group reconfigured, Distributed virtual group renamed.

vNetwork Distributed Switch Event Triggers

VMware provides preconfigured alarms that trigger when events occur on vNetwork Distributed Switches (vDS).

Table 13-15 lists the events you can use to set alarms on a vDS.

Table 13-15. vNetwork Distributed Switch Event Triggers

Event Category	Available Events
vDS creation, modification, and upgrade.	vDS created, Distributed Virtual Switch deleted, vDS reconfigured, vDS upgraded, Upgrade is available, Upgrade is in progress, Cannot complete the upgrade.
vDS port and distributed virtual port group operations	vDS port moved into the distributed virtual port group, vDS moved out of the distributed virtual port group.
Port	Port blocked, Port unblocked, Port connected, Port disconnected, Port created, Port deleted, Port link up, Port link down, Port reconfigured.
Host	Host joined the vDS, Host left the vDS. Host and vCenter Server configuration was synchronized, Host and vCenter Server configuration differs.

Network Event Triggers

VMware provides preconfigured alarms that trigger when events occur on networks.

Table 13-16 lists the events you can use to trigger alarms on networks.

Table 13-16. Network Event Triggers

Event Category	Available Events
dvPort group creation and modification	dvPort group created, dvPort group deleted, dvPort group reconfigured, dvPort group renamed.

Alarm Actions

Alarm actions are operations that occur in response to triggered alarms. For example, email notifications are alarm actions.

VMware provides a list of preconfigured actions you can associate with an alarm. These actions are specific to the object on which you set the alarm. For example, preconfigured alarm actions for hosts include rebooting the host and putting the host in maintenance mode. Alarm actions for virtual machines include powering on, powering off, and suspending the virtual machine.

Although the actions are preconfigured, you must manually set up certain aspects of the action, such as having the action occur when a warning is triggered or when an alert is triggered, and whether to repeat the action.

You can configure alarms to repeat. If you do, alarm actions are repeated at the specified interval (for example, every 10 minutes) until the alarm state changes or the alarm is acknowledged by the administrator

When an alarm is acknowledged, any repeated actions are suppressed. The alarm itself is not reset and remains in the same state until the triggering condition or state is no longer valid, or until an event is received that is configured to reset the state of the alarm.

Some alarm actions, such as sending notification emails or traps, and running a script, require additional configuration.

NOTE The default VMware alarms do not have actions associated with them. You must manually associate actions with the default alarms.

Default vSphere Alarm Actions

VMware provides default alarm actions you can associate with an alarm. When the alarm triggers, the action occurs.

Table 13-17 lists the default vSphere alarm actions.

Table 13-17. Default vSphere Alarm Actions

Action	Description	Alarm Object
Send a notification email	SMTP sends an email message. The SMTP must be ready when the email message is sent. You can set SMTP through vCenter Server or through Microsoft Outlook Express.	datacenter, datastore, cluster, host, resource pool, virtual machine, network, vNetwork distributed switch, dvPort group
Send a notification trap	SNMP sends a notification trap. An SNMP trap viewer is required to view a sent trap. The default hardware health alarms are configured to send SNMP traps.	datacenter, datastore, cluster, host, resource pool, virtual machine
Run a command	Performs the operation defined in the script you specify. It runs as separate process and does not block vCenter Server processes.	datacenter, datastore, cluster, host, resource pool, virtual machine, network, vNetwork distributed switch, dvPort group
Enter or exit maintenance mode	Puts the host in and out of maintenance mode. Maintenance mode restricts virtual machine operations on the host. You put a host in maintenance mode when you need to move or service it.	host
Enter or exit standby	Suspends or resumes the guest operating system on the virtual machine.	host
Reboot or shut down host	Reboots or shuts down the host.	host
Suspend the virtual machine	Suspends the virtual machine when the alarm triggers. You can use the suspend feature to make resources available on a short-term basis or for other situations in which you want to put a virtual machine on hold without powering it down.	virtual machine
Power on or power off the virtual machine	Power on starts the virtual machine and boots the guest operating system if the guest operating system is installed. Power off is analogous to pulling the power cable on a physical machine. It is not a graceful shutdown of the guest operating system, but is used when a shut down might not succeed. For example, a shut down will not work if the guest operating system is not responding.	virtual machine
Reset the virtual machine	Pauses activity on the virtual machine. Transactions are frozen until you issue a Resume command.	virtual machine

Table 13-17. Default vSphere Alarm Actions (Continued)

Action	Description	Alarm Object
Migrate the virtual machine	Powers off the virtual machine and migrates it according to the settings you define when you created the alarm action.	virtual machine
Reboot or shutdown the guest	Reboot shuts down and restarts the guest operating system without powering off the virtual machine. Shutdown shuts down the guest operating system gracefully.	virtual machine

Disabling Alarm Actions

You can disable an alarm action from occurring without disabling the alarm itself. For example, if you have an alarm set to trigger when a host is disconnected, and you put the host in maintenance mode, you can disable the alarm action from firing because you know the host is not available. The alarm is still enabled, so it triggers, but the action does not.

You disable alarm actions for a selected inventory object. You can also disable alarm actions across multiple objects at one time from the object tab. For example, to disable the alarm actions for multiple virtual machines on a host, go to the **Virtual Machines** tab of the host. When you disable the alarm actions for an object, they continue to occur on child objects.

When you disable alarm actions, all actions on all alarms for the object are disabled. You cannot disable a subset of alarm actions.

SNMP Traps as Alarm Actions

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.

When an SNMP trap notification occurs, only one trap is triggered and one notification is sent. Table 13-18 describes the trap information provided in the body of an SNMP notification.

Table 13-18. 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.

NOTE To use SNMP with vCenter Server, you must configure SNMP settings using the vSphere Client.

Email Notifications as Alarm Actions

The SMTP agent included with vCenter Server can be used to send email notifications when alarms are triggered on vCenter Server. When an alarm is triggered, any number of email notification are sent. You define the recipient list when you set up the alarm actions for an alarm.

Table 13-19 describes the information provided in the body of an SMTP notification.

Table 13-19. SMTP 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.`

If the alarm was triggered by an event, the information in Table 13-20 is also included in the body of the email.

Table 13-20. Event Details in Email

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	Datacenter on which the alarm was triggered.
Arguments	Arguments passed with the alarm and their values.

NOTE If you configured SMTP settings in Microsoft Outlook Express, you do not need to configure them for vCenter Server.

Running Scripts as Alarm Actions

You can write scripts and attach them to alarms so that when the alarm triggers, the script runs.

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.

Alarm Environment Variables

To simplify script configuration for alarm actions, VMware provides environment variables for VMware alarms.

Table 13-21 lists the default environment variables defined for alarms. Use these variables to define more complex scripts and attach them to multiple alarms or inventory objects so the action occurs when the alarm triggers.

Table 13-21. Alarm Environment Variables

Variable Name	Variable Description	Supported Alarm Type
VMWARE_ALARM_NAME	Name of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_ID	MOID of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_TARGET_NAME	Name of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_TARGET_ID	MOID of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_OLDSTATUS	Old status of the alarm.	Condition, State, Event
VMWARE_ALARM_NEWSTATUS	New status of the alarm.	Condition, State, Event
VMWARE_ALARM_TRIGGERINGSUMMARY	Multiline summary of the alarm.	Condition, State, Event
VMWARE_ALARM_DECLARINGSUMMARY	Single-line declaration of the alarm expression.	Condition, State, Event
VMWARE_ALARM_ALARMVALUE	Value that triggered the alarm.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	Description text of the alarm status change event.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	Description of the event that triggered the alarm.	Event
VMWARE_ALARM_EVENT_USERNAME	User name associated with the event.	Event
VMWARE_ALARM_EVENT_DATACENTER	Name of the datacenter in which the event occurred.	Event
VMWARE_ALARM_EVENT_COMPUTERESOURCE	Name of the cluster or resource pool in which the event occurred.	Event
VMWARE_ALARM_EVENT_HOST	Name of the host on which the event occurred.	Event
VMWARE_ALARM_EVENT_VM	Name of the virtual machine on which the event occurred.	Event
VMWARE_ALARM_EVENT_NETWORK	Name of the network on which the event occurred.	Event
VMWARE_ALARM_EVENT_DATASTORE	Name of the datastore on which the event occurred.	Event
VMWARE_ALARM_EVENT_DVS	Name of the vNetwork 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, 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 vSphere Client Alarm Actions Configuration dialog box or on a command line.

Table 13-22 lists the command-line substitution parameters for scripts that run as alarm actions.

Table 13-22. Command-Line Parameters for Alarm Action Scripts

Variable	Description
`{eventDescription}`	Text of the alarmStatusChange event. The `{eventDescription}` variable is supported only for Condition and State alarms.
`{targetName}`	Name of the entity on which the alarm is triggered.
`{alarmName}`	Name of the alarm that is triggered.
`{triggeringSummary}`	Summary info of the alarm trigger values.
`{declaringSummary}`	Summary info of the alarm declaration values.
`{oldStatus}`	Alarm status before the alarm is triggered.
`{newStatus}`	Alarm status after the alarm is triggered.
`{target}`	Inventory object on which the alarm is set.

Alarm Reporting

Alarm reporting further restricts when a condition or state alarm trigger occurs by adding a tolerance range and a trigger frequency to the trigger configuration.

Tolerance Range

The tolerance range specifies a percentage above or below the configured threshold point, after which the alarm triggers or clears. A nonzero value triggers and clears the alarm only after the triggering condition falls above or below the tolerance range. A 0 (zero) value triggers and clears the alarm at the threshold point you configured.

vCenter Server uses the following calculation to trigger an alarm:

```
Condition threshold + Tolerance Range = Trigger alarm
```

For example, an alarm is defined to trigger a warning state when a host's CPU usage is above 70%. If you set the tolerance range to 5%, the warning state triggers only when CPU usage is above 75% (70 + 5) and resets to a normal state only when CPU usage falls below 65% (70 - 5).

The tolerance range ensures you do not transition alarm states based on false changes in a condition.

Trigger Frequency

The trigger frequency is the time period during which a triggered alarm action is not reported again. When the time period has elapsed, the alarm action occurs again if the condition or state is still true. By default, the trigger frequency for the default VMware alarms is set to 5 minutes.

For example, if the Host CPU Usage alarm triggers for a warning state at 2 p.m. and an alert state occurs at 2:02 p.m, the alert state is not reported at 2:02 p.m. because the frequency prohibits it. If the warning state is still true at 2:05 p.m., the alarm is reported. This guards against repeatedly reporting insignificant alarm transitions.

Creating Alarms

Creating an alarm involves setting up general alarm settings, alarm triggers, trigger reporting, and alarm actions.

Required Privilege: **Alarms.Create Alarm**

You create an alarm by using the Alarm Settings dialog box. You can open this dialog box by selecting the object in the inventory and using any of the following methods.

- Select **File > New > Alarm**.
- Select **Inventory > *object_type* > Alarm > Add Alarm**.
- Right-click the object and select **Alarm > Add Alarm**.
- In the **Alarms** tab, click the **Definitions** tab, right-click in the pane, and select **New > Alarm**.
- Select the object in the inventory and press Ctrl+A.

Prerequisites

To set up an alarm on an object, the vSphere Client must be connected to a vCenter Server system. In addition, you must have proper user permissions on all relevant objects to create alarms. After an alarm is created, it will be enabled even if the user who created it no longer has permissions.

Procedure

1 Alarm Settings – General on page 169

Use the **General** tab of the Alarm Settings dialog box to set up general alarm information, such as the alarm name, description, monitoring type, and status.

2 Alarm Settings – Triggers on page 170

In the Alarm Settings dialog box, use the **Triggers** tab to add, edit, or remove alarm triggers. The procedure for setting up triggers depends on whether you are setting the trigger for a condition or state or for an event.

3 Alarm Settings – Reporting on page 172

In the Alarm Settings dialog box, use the **Reporting** tab to define a tolerance range and trigger frequency for condition or state triggers. Reporting further restricts when the trigger occurs.

Alarm Settings – General

Use the **General** tab of the Alarm Settings dialog box to set up general alarm information, such as the alarm name, description, monitoring type, and status.

Procedure

1 If necessary, display the Alarm Settings dialog box.

a Display the object in the Inventory panel.

b Select the object and press Ctrl-M.

2 On the **General** tab, enter an alarm name and alarm description.

3 In the Alarm Type box, define the type of alarm to create.

   a In the **Monitor** list, select the object on which to create the alarm.

      The objects in the **Monitor** list are determined by the object selected in the inventory.

   b Select how to monitor the object: for specific conditions or states, or for specific events.

      This determines which triggers are available for the alarm. You can monitor hosts, virtual machines, and datastores for conditions, states, and events. All other objects are monitored only for events.

4 (Optional) To enable the alarm, select **Enable this alarm**.

   You can enable an alarm at anytime after you create it.

5 (Optional) To define the alarm triggers, click the **Triggers** tab.

6 (Optional) To save general edits without updating the alarm triggers or alarm actions, click **OK**.

NOTE You cannot save an alarm if it does not have triggers defined for it.

Alarm Settings – Triggers

In the Alarm Settings dialog box, use the **Triggers** tab to add, edit, or remove alarm triggers. The procedure for setting up triggers depends on whether you are setting the trigger for a condition or state or for an event.

- Set Up a Condition or State Trigger on page 170

  Condition and state triggers monitor performance metrics and object states, such as CPU usage and connection states. You can only monitor hosts, virtual machines, and datastores with condition and state triggers.

- Set Up an Event Trigger on page 171

  Event triggers monitor events that occur on managed objects, vCenter Server, and the License Server. An event is recorded for any action that is of interest to vCenter Server.

Set Up a Condition or State Trigger

Condition and state triggers monitor performance metrics and object states, such as CPU usage and connection states. You can only monitor hosts, virtual machines, and datastores with condition and state triggers.

Procedure

1 If necessary, display the **Triggers** tab of the Alarm Settings dialog box.

   a Display the object in the Inventory panel.

   b Select the object and press Ctrl-M to open the Alarm Settings dialog box.

   c Click the **Triggers** tab.

2 Click **Add**.

   A default condition trigger is added to the triggers list.

3 If you do not want to use the default trigger, replace it.

   a Select the default trigger.

   b Double-click the **Trigger Type** list arrow to open the trigger list.

   c Select a trigger.

4 For a condition trigger, define the condition lengths.

Double-click each attribute field—**Condition**, **Warning**, **Condition Length**, **Alert**, **Condition Length**—and select or enter values. Not all condition triggers have condition lengths.

State triggers occur immediately when the state is reached. You cannot define condition lengths for state alarms.

5 (Optional) Define multiple conditions for the same trigger type.

a Repeat Step 2 through Step 3, and select the same trigger you just configured.

b Set values for each attribute.

6 (Optional) To define additional condition or state triggers, repeat Step 2 through Step 5.

NOTE You cannot use the **VM Total Size on Disk** and **VM Snapshot Size** triggers in combination with other triggers.

---

7 Below the triggers list, select one of the following options to specify how to trigger the alarm.

- If any conditions are satisfied (default).
- If all conditions are satisfied.

8 Click **OK**.

Set Up an Event Trigger

Event triggers monitor events that occur on managed objects, vCenter Server, and the License Server. An event is recorded for any action that is of interest to vCenter Server.

Procedure

1 If necessary, display the **Triggers** tab of the Alarm Settings dialog box.

a Display the object in the Inventory panel.

b Select the object and press Ctrl-M to open the Alarm Settings dialog box.

c Click the **Triggers** tab.

2 Click **Add**.

A default event trigger is added to the triggers list.

3 To replace the default event, double-click the event name and in the **Event** list, select an event.

If you know the event name, you can type it in the Event field to filter the list.

4 To change the default status for the event trigger, double-click the status name and in the **Status** list, select a status.

NOTE To set an alarm to trigger when more than one status has been reached, configure each event status separately. For example, to trigger a warning when a host's hardware health changes and an alert when a host's hardware health changes, configure two Hardware Health Changed events, one with a warning status and one with an alert status.

---

5 (Optional) To configure custom conditions for the event trigger, in the **Condition** column, click **Advanced** to open the Trigger Conditions dialog box.

a Click **Add**.

A default argument is added to the Event Arguments list.

b To replace the default argument, double-click the argument name and in the argument list, select an argument.

c To replace the default operator, double-click the operator name and select an operator from the list.

d Click the Value field and type a value.

e (Optional) To define multiple conditions for the same trigger, repeat Step 5.

f Click **OK**.

6 (Optional) To define additional event triggers, repeat this task.

7 Click **OK**.

Alarm Settings – Reporting

In the Alarm Settings dialog box, use the **Reporting** tab to define a tolerance range and trigger frequency for condition or state triggers. Reporting further restricts when the trigger occurs.

Procedure

1 If necessary, display the **Reporting** tab of the Alarm Settings dialog box.

a Display the object in the Inventory panel.

b Select the object and press Ctrl-M to open the Alarm Settings dialog box.

c Click the **Reporting** tab.

2 Enter a **Tolerance**.

A 0 value triggers and clears the alarm at the threshold point you configured. A non-zero value triggers the alarm only after the condition reaches an additional percentage above or below the threshold point.

```
Condition threshold + Reporting Tolerance = trigger alarm
```

Tolerance values ensure you do not transition alarm states based on false changes in a condition.

3 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.

4 Click **OK**.

Managing Alarms

You can change alarms, disable alarms, reset alarms, and acknowledge triggered alarms. In addition, you can export a list of alarms to a file.

To manage alarms the vSphere Client must be connected to a vCenter Server system.

Acknowledge Triggered Alarms

Acknowledging a triggered alarm suppresses the alarm actions from occurring. It does not reset the alarm to a normal state.

Required privilege: **Alarm.Alarm Acknowledge**

Procedure

1 Display the inventory panel.

2 If necessary, select **View > Status Bar** to display 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**.

5 (Optional) To acknowledge multiple alarms at one time, shift-click each alarm to select it, right-click the selection, and select **Acknowledge Alarm**.

Change Alarm Attributes

You can rename alarms and change alarm triggers, reporting, and actions.

Required privilege: **Alarm.Modify Alarm**

Procedure

1 Display the object in the inventory on which the alarm is defined.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

The Defined in column lists the object on which the alarm is defined. If the value is not **This object**, click the object name. The alarms list for the object opens in the **Alarms** tab.

4 Double-click the alarm to open the Alarm Settings dialog box.

5 Edit the alarm general settings, triggers, reporting, or actions, as needed.

For help on how to configure the values on each tab, click **Help**.

6 Click **OK**.

vCenter Server verifies the configuration of the alarm and updates the alarm for the selected object.

Disable Alarms

You disable alarms from the object on which they were defined. You can enable a disabled alarm at any time.

Required privilege: **Alarm.Modify Alarm**

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

If the Defined in column does not contain **This object** for the alarm to disable, it was not defined on the object selected in the inventory. To open the alarm definitions for that object, click the linked object in the Defined in column.

4 Double-click the alarm to open the Alarm Settings dialog box.

5 Deselect **Enable this alarm**.

6 Click **OK**.

Export a List of Alarms

You can export, to a system file, a list of alarms defined on any managed object in the inventory. The list of alarms for an object includes alarms set on all child objects.

Required privilege: **Read-Only**

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

4 Select **File > Export > Export List**.

5 In the Save As dialog box, specify the directory, file name, and file type for the exported file.

6 Click **Save**.

Identifying Triggered Alarms

You can identify triggered alarms in the vSphere Client Inventory panel, the Status bar, and the **Alarms** tab.

Table 13-23. Triggered Alarm Indicators in the vSphere Client

vSphere Client Location	Triggered Alarm Indicator
Inventory panel	An icon on the object where the alarm was triggered.
Status bar, Triggered Alarms panel	A list of alarms triggered on all inventory objects. Double-click an alarm to select the object in the inventory on which the alarm was triggered.
Alarms tab	A list of alarms triggered on the selected inventory object.

Remove Alarms

You remove alarms from the object on which they were defined. You cannot remove an alarm from a child object that inherited the alarm and you cannot remove the default VMware alarms.

When an alarm is removed, it is removed from vCenter Server and cannot be retrieved.

Required privilege: **Alarm.Remove Alarm**

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

If the Defined in column does not contain **This object** for the alarm to disable, it was not defined on the object selected in the inventory. To open the alarm definitions for that object, click the linked object in the Defined in column.

4 Select the alarm and select **Edit > Remove**.

5 Click **Yes**.

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.

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**.

View Alarms

You view alarms that have been triggered on objects and those that have been defined on objects in the vSphere Client **Alarms** tab.

The **Alarms** tab is available only when the vSphere Client is connected to a vCenter Server system. It has two views, **Triggered Alarms** and **Definitions**.

Triggered Alarms	Lists the alarms triggered on the selected object, including the status of the alarm, the date and time it was last triggered, and if the alarm was acknowledged.
Definitions	Lists the alarms associated with the selected object, including the alarm description and the object on which the alarm was defined.

There vSphere Client offers several different options for viewing alarms.

- View Alarms Defined on an Object on page 175
  The vSphere Client **Alarms** tab contains a list of alarms definitions for the object selected in the inventory.
- View Alarms Triggered on an Object on page 175
  You view triggered alarms on an object on the object's **Alarms** tab.
- View All Alarms Triggered in vCenter Server on page 175
  You view triggered alarms in the **Alarms** tab of the Status bar.

View Alarms Defined on an Object

The vSphere Client **Alarms** tab contains a list of alarms definitions for the object selected in the inventory.

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

The Defined In column displays the object on which the alarm was created.

View Alarms Triggered on an Object

You view triggered alarms on an object on the object's **Alarms** tab.

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Alarms** tab.

3 Click **Triggered Alarms**.

View All Alarms Triggered in vCenter Server

You view triggered alarms in the **Alarms** tab of the Status bar.

Procedure

1 Display the vSphere Client inventory.

2 If necessary, select **View > Status Bar** to display the status pane at the bottom of the vSphere Client.

3 In the Status bar, click **Alarms**.

The list of triggered alarms displays in the status pane.

What to do next

You can also view alarms for a selected inventory object in the Triggered Alarms pane of the **Alarms** tab.

Managing Alarm Actions

You can change alarm actions on the preconfigured vSphere alarms and on custom alarms. Use the vSphere Client to disable alarm actions, identify disabled alarm actions, remove alarm actions, and run commands as alarm actions.

To manage alarm actions, the vSphere Client must be connected to a vCenter Server system.

Disable Alarm Actions

Disabling an alarm action stops the action from occurring when the alarm triggers. It does not disable the alarm from triggering.

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. The alarm actions will continue to fire on the child objects.

Required privilege: **Alarm.Disable Alarm Action**

Procedure

1 Display the object in the inventory.

2 Right-click the object and select **Alarm > Disable Alarm Actions**.

The actions defined for the alarm will not occur on the object until they are enabled.

Enable Alarm Actions

Enabling alarm actions resumes all actions set for triggered alarms.

Required privilege: **Alarm.Disable Alarm Actions**

Procedure

1 Display the object in the inventory on which the alarm is defined.

2 Right-click the object and select **Alarm > Enable Alarm Actions**.

Identifying Disabled Alarm Actions

The vSphere Client uses visual indicators to denote whether alarm actions are enabled or disabled.

When an object is selected in the inventory, you can identify its disabled alarm actions in the following areas of the vSphere user interface:

- In the General pane of the object's **Summary** tab.
- In the Alarm Actions Disabled pane of the **Alarms** tab.
- In the Alarm Actions column of the object's child object tabs. For example, if you select a host in the inventory, the **Virtual Machines** tab displays whether alarm actions are enabled or disabled for each virtual machine on the host.

Remove Alarm Actions

Removing an alarm action stops the action from occurring. It does not stop the alarm itself.

Remove an alarm action if you are certain you will not use again. If you are not sure, disable the alarm action instead.

Required privilege: **Alarm.Remove Alarm**

Procedure

1 Display the object in the inventory on which the alarm is defined.

2 Select the object and click the **Alarms** tab.

3 Click **Definitions**.

4 Right-click the alarm and select **Edit Settings** from the context menu.

If the **Edit Settings** option is not available, the object you selected is not the owner of the alarm. To open the correct object, click the object link in the Defined In column for the alarm. Then repeat this step.

5 In the Alarm Settings dialog box, click the **Actions** tab.

6 Select the action and click **Remove**.

7 Click **OK**.

The alarm action is removed from the alarm.

Run a Command as an Alarm Action

You can run a script when an alarm triggers by configuring a command alarm action.

Required privilege: **Alarm.Modify Alarm**

NOTE Alarm commands run in other processes and do not block vCenter Server from running. They do, however, consume server resources such as processor and memory. This procedure assumes you are adding the alarm action to an existing alarm.

This procedure assumes you are adding the alarm action to an existing alarm.

Procedure

1 If necessary, open the Alarm Settings dialog box.

a Select the object in the inventory on which the alarm is set.

b Click the **Alarms** tab.

c Click **Definitions**.

d Double-click the alarm in the list.

2 Click the **Actions** tab.

3 Click **Add**.

4 Double-click the default action and select **Run a command**.

5 Double-click the **Configuration** field and do one of the following, depending on the command file type:

- If the command is a `.exe` file, enter the full pathname of the command. For example, to run the `cmd.exe` command in the `C:\tools` directory, type:**`c:\tools\cmd.exe`**.
- If the command is a `.bat` file, enter the 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`**.

  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
  ```

  For `.bat` files, the command and its parameters must be formatted into one string.

6 Click **OK**.

When the alarm triggers, the action defined in the script is performed.

Configure SNMP Settings for vCenter Server

To use SNMP with vCenter Server, you must configure SNMP settings using the vSphere Client.

Prerequisites

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 connected 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 "Configure SNMP Management Client Software," on page 135.

Configure vCenter Server SMTP Mail Settings

You can configure vCenter Server to send email notifications as alarm actions.

Prerequisites

Before vCenter Server can send email, you must perform the following tasks:

- Configure the SMTP server settings for vCenter Server or Microsoft Outlook Express.
- Specify email recipients through the Alarm Settings dialog box when you configure alarm actions.

To perform this task, the vSphere Client must be connected to a vCenter Server.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 If the vCenter Server system is part of a connected group, in **Current vCenter Server**, select the vCenter Server system to configure.

3 Select **Mail** in the navigation list.

4 For email message notification, set the SMTP server and SMTP port:

Option	Description
SMTP Server	The DNS name or IP address of the SMTP gateway to use for sending email messages.
Sender Account	The email address of the sender, for example, notifications@example.com.

5 Click **OK**.

Preconfigured VMware Alarms

VMware provides preconfigured alarms for the vCenter Server system that trigger automatically when problems are detected. You only need to set up actions for these alarms. Some alarms are "stateless". vCenter Server does not keep data on stateless alarms and neither computes nor displays their status. Stateless alarms cannot be acknowledged or reset.

Table 13-24 lists the preconfigured alarms available for the vCenter Server system. An asterisk indicates a stateless alarm.

Table 13-24. Default VMware Alarms

Alarm Name	Description
Cannot Connect to Network	Monitors network connectivity on a vSwitch.
Cannot Connect to Storage*	Monitors host or network connectivity to a storage device.
Cluster High Availability Error*	Monitors high availability errors on a cluster.
Datastore Usage On Disk	Monitors datastore disk usage. NOTE This alarm controls the **Status** value for datastores in vSphere Client. If you disable this alarm, the datastore status will be displayed as **Unknown**.
Exit Standby Error*	Monitors whether a host cannot exit standby mode.
Health Status Changed*	Monitors changes to service and extension health status.
Health Status Monitoring	Monitors changes in the overall health status of vCenter Server components.
Host Baseboard Management Controller Status	Monitors the status of the Baseboard Management Controller.
Host Battery Status	Monitors host batteries.

Table 13-24. Default VMware Alarms (Continued)

Alarm Name	Description
Host Connection and Power State	Monitors host connection and power state.
Host Connection Failure*	Monitors host connection failures.
Host CPU Usage	Monitors host CPU usage.
Host Error*	Monitors host error and warning events.
Host Hardware Fan Status	Monitors host fans.
Host Hardware Power Status	Monitors host power.
Host Hardware System Board Status	Monitors host system boards.
Host Hardware Temperature Status	Monitors host temperature.
Host Hardware Voltage	Monitors host voltage.
Host IPMI System Event Log Status	Monitors the capacity of the IPMI System Event Log.
Host Memory Status	Monitors host memory.
Host Memory Usage	Monitors host memory usage.
Host Processor Status	Monitors host processors.
Host Service Console SwapIn Rate	Monitors host service console memory swapin rate.
Host Service Console SwapOut Rate	Monitors host service console memory swapout rate.
Host Status for Hardware Objects	Monitors the status of host hardware objects.
Host Storage Status	Monitors host connectivity to storage devices.
License Error*	Monitors license errors.
License Inventory Monitoring	Monitors the license inventory for compliance.
License User Threshold Monitoring	Monitors the license inventory for compliance.
Migration Error*	Monitors whether a virtual machine cannot migrate or relocate, or is orphaned.
Network Connectivity Lost	Monitors network connectivity on a virtual switch.
Network Uplink Redundancy Degraded*	Monitors network uplink redundancy degradation on a virtual switch.
Network Uplink Redundancy Lost	Monitors network uplink redundancy on a virtual switch.
Non-Compatible Host For Secondary Virtual Machine	Monitors whether there are no compatible hosts available to place a secondary virtual machine.
Non-vSphere Workload Detected on the Datastore	Monitors non-vSphere workloads on a datastore.
Timed Out Starting Secondary Virtual Machine*	Monitors timeouts when starting a Secondary virtual machine.
Virtual Machine CPU Usage	Monitors virtual machine CPU usage.
Virtual machine disk commands canceled	Monitors the number of virtual machine disk commands that are canceled.
Virtual Machine Error*	Monitors virtual machine error and warning events.
Virtual Machine Fault Tolerance State Changed	Monitors changes in fault tolerance state of a virtual machine.
Virtual Machine Fault Tolerance vLockStep Interval Status Changed	Monitors changes in the Fault Tolerance Secondary vLockStep interval.
Virtual Machine High Availability Error*	Monitors high availability errors on a virtual machine.
Virtual Machine Memory Usage	Monitors virtual machine memory usage.

Table 13-24. Default VMware Alarms (Continued)

Alarm Name	Description
Virtual Machine Total Disk Latency	Monitors virtual machine total disk latency.
Virtual Machine Kernel NIC Not Configured Correctly*	Monitors incorrectly configured VMKernel NICs

14 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.

This chapter includes the following topics:

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 ESX 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.

ESX/ESXi System Logs

You might need the ESX/ESXi system log files to resolve technical issues.

Table 14-1 lists log files associated with ESX systems.

Table 14-1. ESX/ESXi System Logs

Component	Location
ESX Server 2.x Service log	`/var/log/vmware/vmware-serverd.log`
ESX Server 3.x or ESX Service log	`/var/log/vmware/hostd.log`
vSphere Client Agent log	`/var/log/vmware/vpx/vpxa.log`
Virtual Machine Kernel Core file	`/root/vmkernel-core.`*`date`* and `/root/vmkernel-log.`*`date`* These files are present after you reboot your machine.
Syslog log	`/var/log/messages`
Service Console Availability report (ESX only)	`/var/log/vmkernel`
VMkernel Messages (ESX only)	`/var/log/vmkernel`
VMkernel Alerts and Availability report (ESX only)	`/var/log/vmkernel`
VMkernel Warning (ESX only)	`/var/log/vmkwarning`
Virtual Machine log file	`vmware.log` in the same directory as the `.vmx` file for the virtual machine
Virtual Machine Configuration file	*`virtual_machine_name`*`/`*`virtual_machine_name`*`.vmx` located on a datastore associated with the managed host. Used the virtual machine summary page in the vSphere Client to determine the datastore on which this file is located.

vSphere Client System Logs

You might need the vSphere Client system log files to resolve technical issues.

Table 14-2 lists log files associated with the vSphere Client machine.

Table 14-2. vSphere Client System Logs

Component	Location
vSphere Client Installation log	Temp directory on the vSphere Client machine. Example: `C:\Documents and Settings\user_name\Local Settings\Temp\vmmsi.log` or `C:\Users\user_name\Local Settings\Temp\vmmsi.log`
vSphere Client Service log	`\vpx` directory in the Application Data directory on the vSphere Client machine. Example: `C:\Documents and Settings\user_name\Local Settings\Application Data\vpx\viclient-x.log` or `C:\Users\user_name\Local Settings\Application Data\vpx\viclient-x.log` `x(=0, 1, ... 9)`

Configure Syslog on ESXi Hosts

All ESX/ESXi hosts run a syslog service (`syslogd`), which logs messages from the VMkernel and other system components to a file.

On an ESXi host, you can use the vSphere Client or the vSphere CLI command `vicfg-syslog` to configure the following options:

Log file path Specifies a datastore path to a file in which syslogd logs all messages.

Remote host Specifies a remote host to which syslog messages are forwarded. In order to receive the forwarded syslog messages, your remote host must have a syslog service installed and correctly configured. Consult the documentation for the syslog service installed on your remote host for information on configuration.

Remote port Specifies the port on which the remote host receives syslog messages.

You cannot use the vSphere Client or `vicfg-syslog` to configure syslog behavior for an ESX host. To configure syslog for an ESX host, you must edit the `/etc/syslog.conf` file.

For more information about `vicfg-syslog`, see the *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Procedure

1 In the vSphere Client inventory, select the host.

2 Click the **Configuration** tab.

3 Click **Advanced Settings**.

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

5 In the **Syslog.Local.DatastorePath** text box, enter the datastore path for the file to which syslog will log messages.

The datastore path should be of the form [*datastorename*] *path_to_file*, where the path is relative to the root of the volume backing the datastore. For example, the datastore path `[storage1] var/log/messages` would map to the path `/vmfs/volumes/storage1/var/log/messages`.

If no path is specified, the default path is `/var/log/messages`.

6 In the **Syslog.Remote.Hostname** text box, enter the name of the remote host to which syslog data will be forwarded.

If no value is specified, no data is forwarded.

7 In the **Syslog.Remote.Port** text box, enter the port on the remote host to which syslog data will be forwarded.

   By default, this option is set to 514, which is the default UDP port used by syslog. Changes to this option take effect only if **Syslog.Remote.Hostname** is configured.

8 Click **OK**.

Changes to the syslog options take effect immediately.

Export Diagnostic Data

You can export all or part of your log file data.

When you export log file data, the `vm-support` script creates a file of the selected data and stores it in a location you specify. The default file type is `.txt` if no other extension is specified. The file contains Type, Time, and Description.

Procedure

1 From the vSphere Client connected to a vCenter Server system or ESX/ESXi host, select **Administration > Export Diagnostic Data**.

2 If the vSphere Client is connected to a vCenter Server system, specify the host whose logs you want to export and the location for storing the log files.

3 If the vSphere Client is connected to an ESX/ESXi host, specify the location for the log files.

4 Click **OK**.

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.

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.

Procedure

- View the log file using one of the following methods.

Task	Description
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 ESX Log Files Using the Service Console

You can collect and package all relevant ESX system and configuration information, a well as ESX log files. This information can be used to analyze the problems.

Procedure

- Run the following script on the service console: `/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**.

ESX/ESXi VMkernel Files

If the VMkernel fails, an error message appears and then the virtual machine reboots. If you specified a VMware core dump partition when you configured your virtual machine, the VMkernel also generates a core dump and error log.

More serious problems in the VMkernel can freeze the machine without an error message or core dump.

Maintaining Your Virtual Infrastructure

Working with Tasks and Events 15

vSphere tasks and events are activities and actions that occur on an object within the vSphere inventory.

This chapter includes the following topics:

Managing Tasks

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

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

NOTE The functionality available in the vSphere Client depends on whether the vSphere Client is connected to a vCenter Server system or an ESX/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 ESX/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.

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.

If you are logged in to a vCenter Server system that is part of a Connected Group, a column in the task list displays the name of the vCenter Server system on which the task was performed.

View All Tasks

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

Procedure

1 Display the object in the inventory.

2 Display the tasks for a single object or the entire vCenter Server.

- To display the tasks for an 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 vCenter Server or an ESX/ESXi host in the vSphere Client **Recent Tasks** pane.

Procedure

1 Display the Inventory panel.

2 Select the object.

3 If necessary, select **View > Status** to display the status bar at the bottom of the vSphere Client.

4 In the status bar, Click **Tasks**.

The list of completed 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.

Procedure

- In the navigation bar, select **Home > Management > Scheduled Tasks**.

Filter Tasks for a Host or Datacenter

Filtering the task list removes tasks performed on child objects.

Procedure

1 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.

Procedure

1 Display the object in the inventory.

2 Select the object and click the **Tasks & Events** tab.

3 If the **Name, Target or Status contains** search field is not displayed, select **View > Filtering**.

4 Click the search field arrow and select the attributes to include in the search.

5 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, and you cannot cancel tasks on an ESX Server version 2.0.1 host.

Required privileges:

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

Prerequisites

To cancel a task, the vSphere Client must be connected to a vCenter Server system.

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 ESX/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 vSphere Client must be connected to a vCenter Server system to create and manage scheduled tasks. The tasks you can schedule are listed in the following table.

Table 15-1. Scheduled Tasks

Scheduled Task	Description
Add a host	Adds the host to the specified datacenter 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.

Table 15-1. Scheduled Tasks (Continued)

Scheduled Task	Description
Deploy a virtual machine	Creates a new virtual machine from a template on the specified host or cluster.
Export a virtual machine	Exports virtual machines that vCenter Server manages to managed formats or hosted formats. The export process converts the source to a virtual machine in the format you specify. This scheduled task is available only when VMware vCenter Converter is installed.
Import a virtual machine	Imports a physical machine, virtual machine, or system image into a virtual machine that vCenter Server manages. This scheduled task is available only when VMware vCenter Converter is installed.
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 VMware vCenter Update Manager is installed.
Remediate	Downloads any new patches discovered during the scan operation and applies the newly configured settings. This task is available only when VMware vCenter 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 VMware Infrastructure 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 Click **OK** to open the Scheduled Task wizard.

6 Enter a task name and task description and click **Next**.

7 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 15-2. 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.

8 Click **Next**.

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

10 Click **Finish**.

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

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 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

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**

Procedure

1 In the vSphere Client navigation bar, 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 navigation bar, 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.

Policy Rules for Task Operations

The vCenter Server and ESX/ESXi hosts adhere to certain rules when managing tasks in the system.

vCenter Server and ESX/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 ESX/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 ESX/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.

Managing Events

An event is an action that occurs on an object in vCenter Server or on a host.

Events include user actions and system actions that occur on managed objects in the vSphere Client inventory. For example, events are created when a user logs in to a virtual machine and when a host connection is lost.

Each event records an event message. An event message is a predefined description of an event. Event messages contain information such as the user who generated the event, the time the event occurred, and the type of event message (information, error, or warning). Event messages are archived in vCenter Server.

Typically, event details include the name of the object on which the event occurred and describes the action that occurred. The object of the event is a link to the object's individual event page.

Note When actions occur on a folder, for example, when an alarm is created on a folder, the related event (in this case the AlarmCreatedEvent) is visible only in the parent datacenter.

Viewing Events

You can view events associated with a single object or with all objects in the vSphere Client inventory.

The events listed for a selected object include events associated with the child objects. Detailed information about a selected event appears in the Event Details panel below the event list.

Note When the vSphere Client is connected directly to an ESX/ESXi host, the **Tasks & Events** tab is labeled **Events**.

View Events Associated with One Object

The events listed for a selected object include events associated with its child objects.

Required privilege: **Read-only**

Procedure

1 Display the object in the vSphere Client inventory.

2 Select the object and click the **Tasks & Events** tab.

3 Click **Events**.

A list of events appears.

4 (Optional) Select an event in the list to see the **Event Details**, including a list of related events and errors in the error stack.

Error messages that display in the Error Stack are shown by default.

5 (Optional) Click the icon next to **Description** to view further details and possible causes of the event.

You can print or save the event details.

View Events Associated with All Objects

The most recent events appear at the top of the Events list. Events are identified by Information type, Error type, and Warning type.

Required privilege: **Read-only**

Procedure

1 View the events associated with all objects in the inventory.

- In the navigation bar, click **Home > Management > Events**.
- In the inventory, select the root node, click the **Tasks & Events** tab, and click **Events**.

2 (Optional) To see details about an event in the list, select the event.

The **Event Details** panel shows the details.

3 (Optional) To see events related to a target object in the list, click the target object's name.

The **Tasks & Events** tab for the selected object appears.

Filter Events on a Host or Datacenter

By default, the events list for an object includes events performed on its child objects. You can remove all child events associated with a host or a datastore and display only the events performed on the object itself.

Procedure

1 Display the host or datacenter in the inventory.

2 Select the host or datacenter and click the **Tasks & Events** tab.

3 Click **Events** to display the events list.

4 If the **Show all entries** list and search field are not visible under the **Tasks** and **Events** buttons, select **View > Filtering**.

5 Click **Show all entries** and select **Show host entries** or **Show datacenter entries**, depending on the object selected.

Use Keywords to Filter the Events List

You can display events based on any attribute, including event name, target, type, user, change history, and time. Filtering is inclusive, not exclusive. If the keyword is found in any of the selected columns, the event is included in the list.

Prerequisites

Required privilege: **Read-only**.

Procedure

1 Select the object on which to filter the events.

- To filter events associated with one object, select the object in the inventory, click the **Events** tab, and click **Events**.
- To filter events associated with all objects, in the navigation bar, click **Home > Management > Events**.

2 If the **Name, Target or Status contains** search field is not visible, select **View > Filtering**.

The search field appears.

3 Click the search field arrow and select the attributes to include in the search.

4 Type a keyword in the field and press Enter.

The events that match the search are retrieved and displayed in the events list.

Trigger an Alarm on an Event

You can configure an alarm to trigger when an event occurs in the vCenter Server System.

Procedure

1 In the inventory, select the object on which to create the alarm.

For example, to create an alarm for all hosts in a cluster, display the cluster. To create an alarm for a single host, display the host.

2 Select **File > New > Alarm**.

3 Complete the information on the **General** tab.

a Enter an alarm name and description.

b In **Alarm Type**, select the object to monitor and select **Monitor for specific events occurring on this object**.

4 Click the **Triggers** tab and set up the alarm triggers.

5 Click to the **Actions** tab and set up the alarm actions.

The vCenter Server verifies the configuration of the alarm and adds the alarm to the list of alarms for the selected object.

For help on configuring the values on each tab, click **Help**.

Export Events

You can export all or part of the events log file when the vSphere Client is connected to a vCenter Server system.

Prerequisites

Required Privilege: **Read-only**

Procedure

1 Select **File > Export > Export Events**.

2 If your vSphere environment has multiple vCenter Servers, in the**vCenter Server** list, select the server where the events occurred.

3 In **File name**, type a name for the event file.

NOTE If you do not specify a file extension, the file is saved as a text file.

4 In **Events**, specify the event attributes on which to filter.

a In **Type**, select **User** or **System**.

b If you selected **User**, select a user option.

- **All users**
- **These users**
- To specify a subset of users, click **Search** and specify the users to include.

c In **Severity**, select the event level: **Error**, **Info**, or **Warning**.

5 In **Time**, specify the time range during which the events to export occurred.

- To specify an hour, day, week, or month time period, select **Last** and set the number and time increment.
- To specify a calendar time span, select **From** and set the from and to dates.

6 In **Limits**, set the number of events to export.

- Select **All matching events**.
- Select **most recent matching events** and enter the number.

7 Click **OK**.

vCenter Server creates the file in the specified location. The file contains the **Type**, **Time**, and **Description** of the events.

Report Errors

Some errors that appear for tasks, events, and in error dialogs can be submitted to VMware for further investigation. In some cases, more information or links to knowledge base articles are provided.

Perform this task in the vSphere Client, within an error dialog, Task Details, or Event Details

Procedure

1 Click **Submit error report** to send the error report.

The Submit Error Report window displays details about the specific error.

2 (Optional) Click the printer icon to print the error log report.

3 (Optional) Click the disk icon to save the error log report.

The error log report can be saved as an HTML file. If you are working offlline, this allows you to use the HTML file to submit the error report to VMware at a later time.

4 Click **Submit**.

The data that appears is sent to VMware in XML format to be analyzed. If found, a relevant VMware Knowledge Base article displays.

Starting and Stopping the vSphere Components

16

You can start and stop each one of the major vSphere components, ESX/ESXi, and vCenter Server. You might want to stop a component to perform maintenance or upgrade operations.

This chapter includes the following topics:

Start an ESX/ESXi Host

When you install ESX/ESXi, it starts itself through the installation reboot process. If your ESX/ESXi host is shut down, you must manually restart it.

Procedure

- On the physical box where ESX/ESXi is installed, press the power button until the power on sequence begins.

The ESX/ESXi host starts, locates its virtual machines, and proceeds with its normal ESX/ESXi functions.

Reboot or Shut Down an ESX/ESXi Host

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

Procedure

1. Shut down all virtual machines running on the ESX/ESXi host.
2. Select the ESX/ESXi host you want to shut down.
3. From the main or right-click menu, select **Reboot** or **Shut Down**.
   - If you select **Reboot**, the ESX/ESXi host shuts down and reboots.
   - If you select **Shut Down**, the ESX/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.

Stop an ESX Host Manually

You can manually shut down an ESX host.

Procedure

1 Log in to the ESX service console.

2 Run the shutdown command.

For example: `shutdown –h now`

ESX shuts down. When it is finished, a message indicates that it is safe to power off your system.

3 Press the power button until the machine powers off.

For information about accessing the service console, see "Connect to the Service Console," on page 26.

Starting vCenter Server

vCenter Server runs as a Windows service. vCenter Server starts when you start the Windows machine on which it is installed. It also restarts when that machine is rebooted.

Verify That vCenter Server Is Running

You can verify that the vCenter Server service is running.

Procedure

1 Go to the Services console for your version of Windows.

For example, select **Control Panel > Administrative Tools > Services** and click **VMware VirtualCenter Server**.

The Status column indicates whether the service started.

2 Right-click the vCenter Server service and select **Properties**.

3 In the VMware vCenter Server Services Properties dialog box, click the **General** tab and view the service status.

Restart the vCenter Server System

The vCenter Server service starts when the machine on which it is installed is booted. You can manually restart the vCenter Server system.

Procedure

1 Go to the Services console for your version of Windows.

For example, select **Control Panel > Administrative Tools > Services** and click **VMware VirtualCenter Server**.

2 Right-click **VMware VirtualCenter Server**, select **Start**, and wait for startup to complete.

3 Close the Properties dialog box.

Stop the vCenter Server System

vCenter Server is a Windows service. You can use the Windows interface to select the service and stop it.

You should not have to stop the vCenter Server service. The vCenter Server should operate without interruption. Continuous operation ensures that all monitoring and task activities are performed as expected.

Procedure

1 Go to the Services console for your version of Windows.

For example, select **Start > Control Panel > Administrative Tools > Services**.

2 Click **VMware VirtualCenter Server Service**.

3 Right-click **VMware VirtualCenter Server**, select **Stop**, and wait for it to stop.

4 Close the Properties dialog box.

Managing Hosts in vCenter Server 17

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 on configuration management of ESX/ESXi hosts, see the *ESX Configuration Guide* or *ESXi Configuration Guide*.

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

See "Add Hosts," on page 62 for information and instructions about adding hosts to vCenter Server.

This chapter includes the following topics:

Disconnecting and Reconnecting a Host

You can disconnect and reconnect a host that is being managed by vCenter Server. Disconnecting a managed host does not remove it from vCenter Server; it temporarily suspends all monitoring activities performed by vCenter Server.

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.

Understanding Managed Host Removal

Removing a managed host from vCenter Server breaks the connection and stops all monitoring and managing functions of that managed host and of all the virtual machines on that managed host. The managed host and its associated virtual machines are removed from the inventory.

Historical data for removed hosts remains in the vCenter Server database.

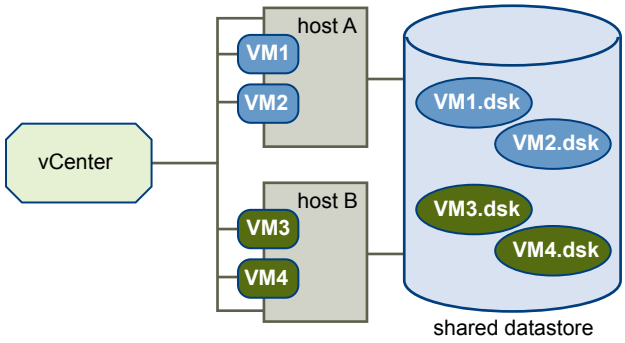
Removing a managed host differs from disconnecting the managed host from vCenter Server. Disconnecting a managed host does not remove it from vCenter Server; it temporarily suspends all vCenter Server monitoring activities. The managed host and its associated virtual machines remain in the vCenter Server inventory.

Removing a managed host from vCenter Server does not remove the virtual machines from the managed host or datastore. It removes only vCenter Server's access to the managed host and virtual machines on that managed host.

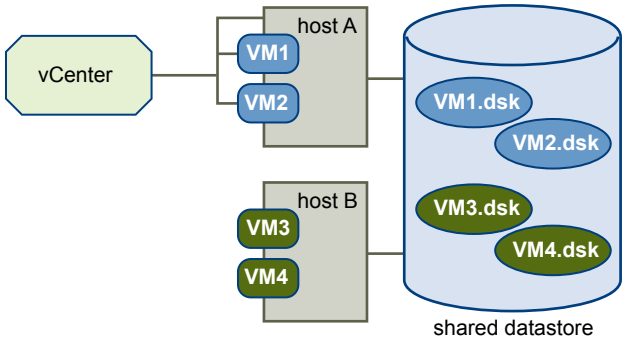
Figure 17-1 illustrates the process for removing a managed host from vCenter Server. In the example here, notice the lost link between vCenter Server and the removed managed host, while the managed host files remain on the datastore.

Figure 17-1. Removing a Host

1. Registered host and virtual machines



2. Remove host. Virtual machines stay on the host's datastore.



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.

18 Migrating Virtual Machines

Migration is the process of moving a virtual machine from one host or storage location to another. Copying a virtual machine creates a new virtual machine. It is not a form of migration.

In vCenter Server, you have the following migration options:

Cold Migration	Moving a powered-off virtual machine to a new host or relocating virtual machine configuration and disk files to new storage locations. Cold migration can be used to migrate virtual machines from one datacenter to another.
Migrating a Suspended Virtual Machine	Moving a suspended virtual machine to a new host or relocating configuration and disk files to new storage locations. You can migrate suspended virtual machines from one datacenter to another.
Migration with vMotion	Moving a powered-on virtual machine to a new host. Migration with vMotion allows you to move a virtual machine to a new host without any interruption in the availability of the virtual machine. Migration with vMotion cannot be used to move virtual machines from one datacenter to another.
Migration with Storage vMotion	Moving the virtual disks or configuration file of a powered-on virtual machine to a new datastore. Migration with Storage vMotion allows you to move a virtual machine's storage without any interruption in the availability of the virtual machine.

Both migration of a suspended virtual machine and migration with vMotion are sometimes referred to as "hot migration", because they allow migration of a virtual machine without powering it off. Migration with vMotion is sometimes referred to as "live migration".

You can move virtual machines manually or set up a scheduled task to perform the cold migration.

This chapter includes the following topics:

- "Limits on Simultaneous Migrations," on page 229

Cold Migration

Cold migration is the migration of a powered-off virtual machine. With cold migration, you have the option of moving the associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

The virtual machine you want to migrate must be powered off prior to beginning the cold migration process.

If a virtual machine is configured to have a 64-bit guest operating system, vCenter Server generates a warning if you try to migrate it to a host that does not support 64-it operating systems. Otherwise, CPU compatibility checks do not apply when you migrate a virtual machine with cold migration.

A cold migration consists of the following tasks:

1. If the option to move to a different datastore was chosen, the configuration files, including the NVRAM file (BIOS settings), and log files are moved from the source host to the destination host's associated storage area. If you chose to move the virtual machine's disks, these are also moved.
2. The virtual machine is registered with the new host.
3. After the migration is completed, the old version of the virtual machine is deleted from the source host if the option to move to a different datastore was chosen.

Migrating a Suspended Virtual Machine

When migrating a suspended virtual machine, you also have the option of moving the associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

When you migrate a suspended virtual machine, the new host for the virtual machine must meet CPU compatibility requirements, because the virtual machine must be able to resume executing instructions on the new host.

Migration of a suspended virtual machine consists of the following steps:

1. The configuration files, including the NVRAM file (BIOS settings), log files, and the suspend file as well as the disks of the virtual machine are moved from the source host to the destination host's associated storage area.
2. The virtual machine is registered with the new host.
3. After the migration is completed, the old version of the virtual machine is deleted from the source host.

Migration with vMotion

Migration with vMotion™ allows virtual machine working processes to continue throughout a migration.

The entire state of the virtual machine, as well as its configuration file, if necessary, is moved to the new host, while the associated virtual disk remains in the same location on storage that is shared between the two hosts. After the virtual machine state is migrated to the alternate host, the virtual machine runs on the new host.

The state information includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes transaction data and whatever bits of the operating system and applications are in the memory. The defining and identification information stored in the state includes all the data that maps to the virtual machine hardware elements, such as BIOS, devices, CPU, MAC addresses for the Ethernet cards, chip set states, registers, and so forth.

When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements in order for the migration to proceed.

Migration with vMotion happens in three stages:

1 When the migration with vMotion is requested, vCenter Server verifies that the existing virtual machine is in a stable state with its current host.

2 The virtual machine state information (memory, registers, and network connections) is copied to the target host.

3 The virtual machine resumes its activities on the new host.

If any error occurs during migration, the virtual machines revert to their original states and locations.

Migration of a suspended virtual machine and migration with vMotion can be referred to as hot migration, because they allow migration of a virtual machine without powering it off.

Host Configuration for vMotion

In order to successfully use vMotion, you must first configure your hosts correctly.

Ensure that you have correctly configured your hosts in each of the following areas:

- Each host must be correctly licensed for vMotion.
- Each host must meet shared storage requirements for vMotion.
- Each host must meet the networking requirements for vMotion.

vMotion Shared Storage Requirements

Configure hosts for vMotion with shared storage to ensure that virtual machines are accessible to both source and target hosts.

During a migration with vMotion, the migrating virtual machine must be on storage accessible to both the source and target hosts. Ensure that the hosts configured for vMotion use shared storage. Shared storage is typically on a storage area network (SAN), but can also be implemented using iSCSI and NAS shared storage. See the VMware *SAN Configuration Guide* for additional information on SAN and the *ESX Configuration Guide* or *ESXi Configuration Guide* for information on other shared storage.

vMotion Networking Requirements

Migration with vMotion requires correctly configured network interfaces on source and target hosts.

vMotion requires a Gigabit Ethernet (GigE) network between all vMotion-enabled hosts. Each host enabled for vMotion must have a minimum of two Ethernet adapters, at least one of which must be a GigE adapter.

Recommended networking best practices are as follows:

- Use one dedicated Ethernet adapter for the service console (on ESX hosts).
- Use one dedicated GigE adapter for vMotion.
- If only two Ethernet adapters are available:
  - For best security, dedicate the GigE adapter to vMotion, and use VLANs to divide the virtual machine and management traffic on the other adapter.
  - For best availability, combine both adapters into a bond, and use VLANs to divide traffic into networks: one or more for virtual machine traffic, one for the service console (on ESX hosts), and one for vMotion.

Configure the virtual networks on vMotion-enabled hosts as follows:

- On each host, configure a VMkernel port group for vMotion.
- Ensure that virtual machines have access to the same subnets on source and destination hosts.

- If you are using vSwitches for networking, ensure that the network labels used for virtual machine port groups are consistent across hosts. During a migration with vMotion, vCenter Server assigns virtual machines to port groups based on matching network labels.

  NOTE You cannot migrate virtual machines that are attached to a virtual intranet with vMotion, even if the destination host has a virtual intranet configured with the same network label.

- If you are using vNetwork Distributed Switches for networking, ensure that source and destination hosts are members of all vNetwork Distributed Switches that virtual machines use for networking.
- Use of Jumbo Frames is recommended for best vMotion performance.

Virtual Machine Configuration Requirements for vMotion

A number of specific virtual machine configurations can prevent migration of a virtual machine with vMotion.

The following virtual machine configurations can prevent migration with vMotion:

- You cannot use migration with vMotion to migrate virtual machines using raw disks for clustering purposes.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host. (For example, you cannot migrate a virtual machine with a CD drive backed by the physical CD drive on the source host.) Disconnect these devices before migrating the virtual machine.

  Virtual machines with USB passthrough devices can be migrated with vMotion as long as the devices are enabled for vMotion.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer. Disconnect these devices before migrating the virtual machine.

Swapfile Location Compatibility

Virtual machine swapfile location affects vMotion compatibility in different ways depending on the version of ESX/ESXi running on the virtual machine's host.

Virtual machines on hosts running ESX Server 3.0.x have a virtual machine swap file located with the virtual machine configuration file. Virtual machines on these hosts can be migrated with vMotion only if the destination host can access the VMFS volume where the swap file is located.

You can configure ESX 3.5 or ESXi 3.5 or later hosts to store virtual machine swapfiles in one of two locations: with the virtual machine configuration file, or on a local swapfile datastore specified for that host. You can also set individual virtual machines to have a different swapfile location from the default set for their current host.

The location of the virtual machine swapfile affects vMotion compatibility as follows:

- Migrations between hosts running ESX/ESXi version 3.5 and later: Migrations with vMotion and migrations of suspended and powered-off virtual machines are allowed.

  During a migration with vMotion, if the swapfile location specified on the destination host differs from the swapfile location specified on the source host, the swapfile is copied to the new location. This can result in slower migrations with vMotion. If the destination host cannot access the specified swapfile location, it stores the swapfile with the virtual machine configuration file.
- Migrations between a host running ESX/ESXi version 3.5 and later and a host running an earlier version of ESX Server: Migrations of suspended and powered-off virtual machines are allowed. If the virtual machine is configured to use a local swapfile datastore, attempting to migrate it to a host that does not support this configuration produces a warning, but the migration can proceed. When the virtual machine is powered on again, the swapfile is located with the virtual machine.

Migrations with vMotion are not allowed unless the destination swapfile location is the same as the source swapfile location. In practice, this means that virtual machine swapfiles must be located with the virtual machine configuration file.

See the vSphere Client online Help for more information on configuring swapfile policies.

Migrating Virtual Machines with Snapshots

Migration of virtual machines with snapshots is possible if the virtual machine resides on shared storage accessible to source and destination hosts.

Some restrictions apply when migrating virtual machines with snapshots. You cannot migrate a virtual machine with snapshots with Storage vMotion. Otherwise, migrating a virtual machine with snapshots is permitted, regardless of the virtual machine power state, as long as the virtual machine is being migrated to a new host without moving its configuration file or disks. (The virtual machine must reside on shared storage accessible to both hosts.)

If the migration involves moving the configuration file or virtual disks, the following additional restrictions apply:

- The starting and destination hosts must be running ESX 3.5 or ESXi 3.5 or later.
- All of the virtual machine files and disks must reside in a single directory, and the migrate operation must move all the virtual machine files and disks to a single destination directory.

Reverting to a snapshot after migration with vMotion might cause the virtual machine to fail, because the migration wizard cannot verify the compatibility of the virtual machine state in the snapshot with the destination host. Failure occurs only if the configuration in the snapshot uses devices or virtual disks that are not accessible on the current host, or if the snapshot contains an active virtual machine state that was running on hardware that is incompatible with the current host CPU.

Migration with Storage vMotion

Using Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running.

You can choose to place the virtual machine and all its disks in a single location, or select separate locations for the virtual machine configuration file and each virtual disk. The virtual machine does not change execution host during a migration with Storage vMotion.

During a migration with Storage vMotion, you can transform virtual disks from thick-provisioned to thin-provisioned or from thin-provisioned to thick-provisioned.

Storage vMotion has a number of uses in administering virtual infrastructure, including the following examples of use:

- Upgrading datastores without virtual machine downtime. You can migrate running virtual machines from a VMFS2 datastore to a VMFS3 datastore, and upgrade the VMFS2 datastore without any impact on virtual machines. You can then use Storage vMotion to migrate virtual machines back to the original datastore without any virtual machine downtime.
- Storage maintenance and reconfiguration. You can use Storage vMotion to move virtual machines off of a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.
- Redistributing storage load. You can use Storage vMotion to manually redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Storage vMotion Requirements and Limitations

A virtual machine and its host must meet resource and configuration requirements for the virtual machine disks to be migrated with Storage vMotion.

Storage vMotion is subject to the following requirements and limitations:

- Virtual machines with snapshots cannot be migrated using Storage vMotion.
- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thin-provisioned disks during migration as long as the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.
- Migration of virtual machines during VMware Tools installation is not supported.
- The host on which the virtual machine is running must have a license that includes Storage vMotion.
- ESX/ESXi 3.5 hosts must be licensed and configured for vMotion. ESX/ESXi 4.0 and later hosts do not require vMotion configuration in order to perform migration with Storage vMotion.
- The host on which the virtual machine is running must have access to both the source and target datastores.
- For limits on the number of simultaneous migrations with vMotion and Storage vMotion, see "Limits on Simultaneous Migrations," on page 229.

CPU Compatibility and EVC

vCenter Server performs a number of compatibility checks before allowing migration of running or suspended virtual machines to ensure that the virtual machine is compatible with the target hosts.

vMotion transfers the running state of a virtual machine between underlying ESX/ESXi systems. Successful migration requires that the processors of the target host be able to execute using the equivalent instructions that the processors of the source host were using when the virtual machine was migrated off of the source host. Processor clock speeds and cache sizes, and the number of processor cores can vary, but processors must come from the same vendor class (AMD or Intel) and use compatible feature sets to be compatible for migration with vMotion.

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 there are compatibility problems that will prevent migration.

When a virtual machine is powered on, it determines its available CPU feature set. The virtual machine's CPU feature set is based on the host's CPU feature set. However, some of the host CPU features can be hidden from the virtual machine if the host is part of a cluster using Enhanced vMotion Compatibility (EVC), or if a CPU compatibility mask is applied to the virtual machine.

NOTE 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*.

CPU Compatibility Scenarios

vCenter's CPU compatibility checks compare the features available on the source and target host CPUs. A mismatch in user-level features blocks migration. A mismatch in kernel-level features does not block migration unless the virtual machine might execute instructions that are unavailable on the destination host.

User-level features are non-privileged instructions that might be used by virtual machine applications. These include SSE3, SSSE3, SSE4.1, SSE4.2, and AES. Because they are user-level instructions that bypass the virtualization layer, these instructions could cause application instability if mismatched after a migration with vMotion.

Kernel-level features are privileged instructions that might be used by the virtual machine operating system. These include the AMD No eXecute (NX) and the Intel eXecute Disable (XD) security features.

When you attempt to migrate a virtual machine with vMotion, one of the following scenarios applies:

- The destination host feature set matches the virtual machine's CPU feature set. CPU compatibility requirements are met, and migration with vMotion proceeds.
- The virtual machine's CPU feature set contains features not supported by the destination host. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.
- The destination host supports the virtual machine's feature set, plus additional user-level features (such as SSE4.1) not found in the virtual machine's feature set. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.
- The destination host supports the virtual machine's feature set, plus additional kernel-level features (such as NX or XD) not found in the virtual machine's feature set. CPU compatibility requirements are met, and migration with vMotion proceeds. The virtual machine retains its CPU feature set as long as it remains powered on, allowing it to migrate freely back to the original host. However, if the virtual machine is rebooted, it acquires a new feature set from the new host, which might cause vMotion incompatibility if you attempt to migrate the virtual machine back to the original host.

CPU Families and Feature Sets

Processors are grouped into families. Processors within a given family generally have similar feature sets.

Processor families are defined by the processor vendors. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features. In some cases, processor vendors have introduced significant architectural changes within the same processor family, such as the SSSE3 and SSE4.1 instructions, and NX/XD CPU security features.

By default, vCenter Server identifies mismatches on features accessible to applications as incompatible to guarantee the stability of virtual machines after migrations with vMotion.

Server hardware's CPU specifications will usually indicate whether or not the CPUs contain the features that affect vMotion compatibility. If the specifications of a server or its CPU features are unknown, VMware's bootable CPU identification utility (available for download from the VMware website) can be used to boot a server and determine whether its CPUs contain features such as SSE3, SSSE3, and NX/XD.

For more information on identifying Intel processors and their features, see *Application Note 485: Intel® Processor Identification and the CPUID Instruction*, available from Intel. For more information on identifying AMD processors and their features, see *CPUID Specification*, available from AMD.

About Enhanced vMotion Compatibility

You can use the Enhanced vMotion Compatibility (EVC) feature to help ensure vMotion compatibility for the hosts in a cluster. 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. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs.

Configure EVC from the cluster settings dialog box. When you configure EVC, you configure all host processors in the cluster to present the feature set of a baseline processor. This baseline feature set is called the EVC mode. EVC leverages AMD-V Extended Migration technology (for AMD hosts) and Intel FlexMigration technology (for Intel hosts) to mask processor features so that hosts can present the feature set of an earlier generation of processors. The EVC mode must be equivalent to, or a subset of, the feature set of the host with the smallest feature set in the cluster.

EVC masks only those processor features that affect vMotion compatibility. Enabling EVC does not prevent a virtual machine from taking advantage of faster processor speeds, increased numbers of CPU cores, or hardware virtualization support that might be available on newer hosts.

EVC cannot prevent virtual machines from accessing hidden CPU features in all circumstances. Applications that do not follow CPU vendor recommended methods of feature detection might behave unexpectedly in an EVC environment. VMware EVC cannot be supported with ill-behaved applications that do not follow the CPU vendor recommendations. For more information about creating well-behaved applications, search the VMware Knowledge Base for the article *Detecting and Using New Features in CPUs*.

EVC Requirements

Hosts in an EVC cluster must meet certain requirements.

To enable EVC on a cluster, the cluster must meet the following requirements:

- All virtual machines in the cluster that are running on hosts with a feature set greater than the EVC mode you intend to enable must be powered off or migrated out of the cluster before EVC is enabled. (For example, consider a cluster containing an Intel Xeon Core 2 host and an Intel Xeon 45nm Core 2 host, on which you intend to enable the Intel Xeon Core 2 baseline. The virtual machines on the Intel Xeon Core 2 host can remain powered on, but the virtual machines on the Intel Xeon 45nm Core 2 host must be powered off or migrated out of the cluster.)
- All hosts in the cluster must have CPUs from a single vendor, either AMD or Intel.
- All hosts in the cluster must be running ESX/ESXi 3.5 Update 2 or later.
- All hosts in the cluster must be connected to the vCenter Server system.
- All hosts in the cluster must have advanced CPU features, such as hardware virtualization support (AMD-V or Intel VT) and AMD No eXecute (NX) or Intel eXecute Disable (XD), enabled in the BIOS if they are available.
- All hosts in the cluster should be configured for vMotion. See "Host Configuration for vMotion," on page 213.
- All hosts in the cluster must have supported CPUs for the EVC mode you want to enable. Table 18-1 lists the processor families supported for each EVC mode. To check EVC support for a specific processor or sever model, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

Any host added to an existing EVC-enabled cluster must also meet the requirements

NOTE Hardware vendors sometimes disable particular CPU features in the BIOS by default. This can cause problems in enabling EVC, because the EVC compatibility checks detect the absence of features that are expected to be present for a particular CPU. If you cannot enable EVC on a system with a compatible processor, ensure that all features are enabled in the BIOS.

Table 18-1 lists the processors supported in EVC Clusters.

Table 18-1. Processors Supported in EVC Clusters

Vendor	EVC Mode	Processors Supported
AMD	AMD Opteron Generation 1	AMD Opteron Generation 1
		AMD Opteron Generation 2
		AMD Opteron Generation 3
	AMD Opteron Generation 2	AMD Opteron Generation 2
		AMD Opteron Generation 3
	AMD Opteron Generation 3	AMD Opteron Generation 3
	AMD Opteron Generation 3* (No 3DNow!)	AMD Opteron Generation 3
Intel	Intel Xeon Core 2	Intel Xeon Core 2
		Intel Xeon 45nm Core 2
		Intel Xeon Core i7
		Intel Xeon 32nm Core i7
	Intel Xeon 45nm Core 2	Intel Xeon 45nm Core 2
		Intel Xeon Core i7
		Intel Xeon 32nm Core i7
	Intel Xeon Core i7	Intel Xeon Core i7
		Intel Xeon 32nm Core i7
	Intel Xeon 32nm Core i7	Intel Xeon 32nm Core i7

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

Before you create an EVC cluster, ensure that the hosts you intend to add to the cluster meet the requirements listed in "EVC Requirements," on page 218.

Procedure

1 Create an empty cluster, and enable EVC.

Select the CPU vendor and EVC mode appropriate for the hosts you intend to add to the cluster. For information on configuring EVC, see the vSphere Client online Help.

Other cluster features such as VMware DRS and VMware 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.

2 Select a host to move into the cluster.

3 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.

4 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.

5 Repeat Step 3 and Step 4 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

Before you enable EVC on an existing cluster, ensure that the hosts in the cluster meet the requirements listed in "EVC Requirements," on page 218.

Procedure

1 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

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 221.

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**.

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 machines does not make use of any additional CPU features exposed by the new EVC mode of the cluster 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 has been set to the Intel Xeon Core™ 2 EVC mode. A virtual machine powered on in this cluster runs in the Intel Xeon Core 2 EVC mode. If the cluster EVC mode is raised to Intel Xeon 45nm Core 2, the virtual machine remains at the lower Intel 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 for a cluster or a host to determine the EVC modes of the running virtual machines.

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!

Future generations of AMD processors might not include 3DNow!™ CPU instructions. vCenter Server 4.1 provides an EVC mode that masks the 3DNow! instructions from virtual machines, allowing you to prepare clusters for the introduction of AMD hosts without 3DNow! instructions.

Processors without the 3DNow! instructions will not be vMotion-compatible with older processors that have the 3DNow! instructions, unless an EVC mode or CPU compatibility mask is used to mask these instructions.

The **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 these clusters to maintain vMotion compatibility with future AMD Opteron hosts that might 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

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.

CPU Compatibility Masks

CPU compatibility masks allow per-virtual machine customization of the CPU features visible to a virtual machine.

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 migrations with vMotion.

Default values for the CPU compatibility masks are set by VMware to guarantee the stability of virtual machines after a migration with vMotion.

In some cases, where a choice between CPU compatibility or guest operating system features (such as NX/XD) exists, VMware provides check-box options to configure individual virtual machines through the virtual machine's Advanced Settings option. For more control over the visibility of CPU features, you can edit the virtual machine's CPU compatibility mask at the bit level.

CAUTION Manual edit of the CPU compatibility masks without the appropriate documentation and testing might lead to an unsupported configuration.

CPU compatibility masks cannot prevent virtual machines from accessing masked CPU features in all circumstances. In some circumstances, applications can detect and use masked features even though they are hidden from the guest operating system. In addition, on any host, applications that use unsupported methods of detecting CPU features rather than using the CPUID instruction can access masked features. Virtual machines running applications that use unsupported CPU detection methods might experience stability problems after migration.

Migrate a Powered-Off or Suspended Virtual Machine

You can use the Migration wizard to migrate a powered-off virtual machine or suspended virtual machine.

Procedure

1 Display the virtual machine you want to migrate in the inventory.

2 Right-click on the virtual machine and select **Migrate** from the pop-up menu.

3 Select whether to change the virtual machine's host, datastore, or both.

Option	Description
Change host	Move the virtual machine to another host.
Change datastore	Move the virtual machine's configuration file and virtual disks.
Change both host and datastore	Move the virtual machine to another host and move its configuration file and virtual disks.

4 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.

5 Select the destination resource pool for the virtual machine migration and click **Next**.

6 If you chose to move the virtual machine's configuration file and virtual disks, select the destination datastore.

- To move the virtual machine configuration files and virtual disks to a single destination, select the datastore and click **Next**.
- To select individual destinations for the configuration file and each virtual disk, click **Advanced**. In the **Datastore** column, select a destination for the configuration file and each virtual disk, and click **Next**.

7 If you chose to move the virtual machine's configuration file and virtual disks, select a disk format and click **Next**.

Option	Description
Same as Source	Use the format of the original virtual disk. If you select this option for an RDM disk in physical compatibility mode, only the mapping file is migrated. If you select this option for an RDM disk in virtual compatibility mode, the RDM is converted to a 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 grow in size up to its maximum allocated capacity. This option is not available for RDMs in physical compatibility mode. If you select this option for a virtual compatibility mode RDM, the RDM is converted to a thin virtual disk. RDMs converted to virtual disks cannot be converted back to RDMs.
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. This option is not available for RDMs in physical compatibility mode. If you select this option for a virtual compatibility mode RDM, the RDM is converted to a virtual disk. RDMs converted to virtual disks cannot be converted back to RDMs.

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.

8 Review the summary 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.

Migrate a Powered-On Virtual Machine with vMotion

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.

- "Host Configuration for vMotion," on page 213
- "Virtual Machine Configuration Requirements for vMotion," on page 214

Procedure

1 Display the virtual machine 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 individual 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

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 Display the virtual machine 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 resource pool and click **Next**.

5 Select the destination datastore.

- To move the virtual machine configuration files and virtual disks to a single destination, select the datastore and click **Next**.
- To select individual destinations for the configuration file and each virtual disk, click **Advanced**. In the **Datastore** column, select a destination for the configuration file and each virtual disk, and click **Next**.

6 Select a disk format and click **Next**:

Option	Description
Same as Source	Use the format of the original virtual disk. If you select this option for an RDM disk in physical compatibility mode, only the mapping file is migrated. If you select this option for an RDM disk in virtual compatibility mode, the RDM is converted to a 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 grow in size up to its maximum allocated capacity. This option is not available for RDMs in physical compatibility mode. If you select this option for a virtual compatibility mode RDM, the RDM is converted to a thin virtual disk. RDMs converted to virtual disks cannot be converted back to RDMs.
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. This option is not available for RDMs in physical compatibility mode. If you select this option for a virtual compatibility mode RDM, the RDM is converted to a virtual disk. RDMs converted to virtual disks cannot be converted back to RDMs.

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 choose to leave a disk in its original location, the disk format is not converted, regardless of the selection made here.

7 Review the page and click **Finish**.

A task is created that begins the virtual machine migration process.

About Migration Compatibility Checks

During migration, the Migrate Virtual Machine wizard checks the destination host for compatibility with the migrating virtual machine using a number of criteria.

When you select a host, the **Compatibility** panel at the bottom of the Migrate Virtual Machine wizard displays information about the compatibility of the selected host or cluster with the virtual machine's configuration.

If the virtual machine is compatible, the panel displays the message, `Validation succeeded`. If the virtual machine is not compatible with either the host's or cluster's configured networks or datastores, the compatibility window can display both warnings and errors:

- Warning messages do not disable migration. Often the migration is justified and you can continue with the migration despite the warnings.
- Errors can disable migration if there are no error-free destination hosts among the selected destination hosts. In this case, the **Next** button is disabled.

For clusters, the network and datastore configurations are taken into account when checking compatibility issues. For hosts, the individual host's configuration is used. A possible problem might be that vMotion is not enabled on one or both hosts.

A specific host CPU feature's effects on compatibility are dependent on whether ESX/ESXi exposes or hides them from virtual machines.

- Features that are exposed to virtual machines are not compatible when they are mismatched.
- Features that are not exposed to virtual machines are compatible regardless of mismatches.

Specific items of virtual machine hardware can also cause compatibility issues. For example, a virtual machine using an enhanced vmxnet virtual NIC cannot be migrated to a host running a version of ESX that does not support enhanced vmxnet.

Storage vMotion Command-Line Syntax

In addition to using the Migration wizard, you can initiate migrations with Storage vMotion from the vSphere Command-Line Interface (vSphere CLI) using the `svmotion` command.

For more information about installing and using the vSphere CLI, see *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

You can run the `svmotion` command in either interactive or noninteractive mode.

- To use the command in interactive mode, type **`svmotion --interactive`**. You are prompted for all the information necessary to complete the storage migration. When the command is invoked in interactive mode, all other parameters given are ignored.
- In noninteractive mode, the `svmotion` command uses the following syntax:

```
svmotion [Standard CLI options] --datacenter=datacenter_name --vm
'VM_config_datastore_path:new_datastore' [--disks
'virtual_disk_datastore_path:new_datastore, virtual_disk_datastore path:new_datastore]'
```

Square brackets indicate optional elements.

On Windows systems, use double quotes instead of single quotes around the values specified for the `--vm` and `--disks` options.

For more information on the standard CLI options, see the *vSphere Command-Line Interface Installation and Scripting Guide* and *vSphere Command-Line Interface Reference*.

Table 18-2 describes the parameters for the `svmotion` command.

Table 18-2. svmotion Command Parameters

Parameter	Description
datacenter	The datacenter that contains the virtual machine to be migrated. You must quote the name if it contains white space or other special characters.
VM_config_datastore path	The datastore path to the virtual machine's configuration file. If the path contains white space or other special characters, you must quote it.
new_datastore	The name of the new datastore to which the virtual machine configuration file or disk is to be moved. Do not include brackets around the name of the new datastore.
`--disks`	If you do not specify this parameter, all virtual disks associated with a virtual machine are relocated to the same datastore as the virtual machine configuration file. By specifying this parameter, you can choose to locate individual virtual disks to different datastores. To keep a virtual disk on its current datastore, use the `--disks` option for that disk with its current datastore as the *new_datastore*.
virtual_disk_datastore_path	The datastore path to the virtual disk file.

Determine the Path to a Virtual Machine Configuration File

The path to the virtual machine configuration file is a necessary argument to the `svmotion` command.

You must specify the datastore path to the virtual machine's configuration file in the *`VM_config_datastore_path`* `svmotion` command.

Procedure

1 In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

2 Click **Edit Settings** to display the Virtual Machine Properties dialog box.

3 Click the **Options** tab, and select **General Options**.

The path to the virtual machine configuration file appears in the **Virtual Machine Configuration File** text box.

Determine the Path to a Virtual Disk File

You must specify the virtual disk datastore path as part of the `svmotion` command.

Procedure

1 In the vSphere Client inventory, select the virtual machine to which the virtual disk belongs, and click the **Summary** tab.

2 Click **Edit Settings** to display the Virtual Machine Properties dialog box.

3 Click the **Hardware** tab, and select the virtual disk from the list of devices.

The path to the virtual disk file appears in the **Disk File** text box.

Storage vMotion Examples

The examples show how to use the Storage vMotion command-line interface to relocate a virtual machine and all its disks, or to relocate the virtual machine configuration file while leaving the disks in place.

The examples in this section are formatted on multiple lines for readability. The command should be issued on a single line.

An example of relocating all of a virtual machine's disks to a datastore named `new_datastore`:

```
svmotion --url=https://myvc.mycorp.com/sdk
         --username=me
         --password=secret
         --datacenter=DC1
         --vm='[old_datastore] myvm/myvm.vmx: new_datastore'
```

An example of relocating a virtual machine to `new_datastore`, while leaving the disks, `myvm_1.vmdk` and `myvm_2.vmdk` on `old_datastore`:

```
svmotion --datacenter='My DC'
         --vm='[old_datastore] myvm/myvm.vmx:
               new_datastore'
         --disks='[old_datastore] myvm/myvm_1.vmdk:
                  old_datastore,
                  [old_datastore] myvm/myvm_2.vmdk:
                  old_datastore'
```

Limits on Simultaneous Migrations

vCenter Server places limits on the number of simultaneous virtual machine migration and provisioning operations that can occur on each host, network, and datastore.

Each operation, such as a migration with vMotion or cloning a virtual machine, is assigned a resource cost. Each type of resource, such as host, datastore, or network, has a maximum cost that it can support at any one time. Any new migration or provisioning operation that would cause a resource to exceed its maximum cost does not proceed immediately, but is queued until other operations complete and release resources. Each of the network, datastore, and host limits must be satisfied in order for the operation to proceed.

Network Limits

Network limits apply to migrations with vMotion only. Network limits depend on both the version of ESX/ESXi and the network type.

Table 18-3 lists network limits for migration with vMotion.

Table 18-3. Network Limits for Migration with vMotion

Operation	ESX/ESXi Version	Network Type	Maximum Cost
vMotion	3.x	1GigE and 10GigE	2
vMotion	4.0	1GigE and 10GigE	2
vMotion	4.1	1GigE	4
vMotion	4.1	10GigE	8

All migrations with vMotion have a network resource cost of 1.

Datastore Limits

Datastore limits apply to migrations with vMotion and with Storage vMotion. A migration with vMotion involves one access to the datastore. A migration with storage vMotion involves one access to the source datastore and one access to the destination datastore.

Table 18-4 lists datastore limits for migration with vMotion and Storage vMotion. Table 18-5 lists the datastore resource costs for migration with vMotion and Storage vMotion.

Table 18-4. Datastore Limits for Migration with vMotion and Storage vMotion

Operation	ESX/ESXi Version	Maximum Cost
vMotion/Storage vMotion	3.x	8
vMotion/Storage vMotion	4.0	8
vMotion/Storage vMotion	4.1	128

Table 18-5. Datastore Resource Costs for vMotion and Storage vMotion

Operation	ESX/ESXi Version	Datastore Resource Cost
vMotion	3.x	1
vMotion	4.0	1
vMotion	4.1	1
Storage vMotion	3.x	1

Table 18-5. Datastore Resource Costs for vMotion and Storage vMotion (Continued)

Operation	ESX/ESXi Version	Datastore Resource Cost
Storage vMotion	4.0	1
Storage vMotion	4.1	16

Host Limits

Host limits apply to migrations with vMotion, Storage vMotion, and other provisioning operations such as cloning, deployment, and cold migration.

Table 18-6 lists the host limits for migrations with vMotion, migrations with Storage vMotion, and provisioning operations. Table 18-7 lists the host resource cost for these operations.

Table 18-6. Host Limits for vMotion, Storage vMotion, and Provisioning Operations

Operation	ESX/ESXi Version	Maximum Cost
vMotion	3.x, 4.0, 4.1	8
Storage vMotion	3.x, 4.0, 4.1	8
other provisioning operations	3.x, 4.0, 4.1	8

Table 18-7. Host Resource Costs for vMotion, Storage vMotion, and Provisioning Operations

Operation	ESX/ESXi Version	Host Resource Cost
vMotion	3.x	4
vMotion	4.0	4
vMotion	4.1	1
Storage vMotion	3.x	4
Storage vMotion	4.0	4
Storage vMotion	4.1	4
other provisioning operations	3.x, 4.0, 4.1	1

Using vCenter Maps 19

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

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.

vCenter vMotion Maps

vMotion resource maps provide a visual representation of hosts, datastores, and networks associated with the selected virtual machine.

vMotion resource maps also indicate which hosts in the virtual machine's cluster or datacenter are compatible with the virtual machine and are potential migration targets. For a host to be compatible, it must meet the following criteria.

- Connect to all the same datastores as the virtual machine.
- Connect to all the same networks as the virtual machine.
- Have compatible software with the virtual machine.
- Have a compatible CPU with the virtual machine.

NOTE The vMotion map provides information as to whether vMotion might be possible, and if not, what an administrator might do to remedy the situation. It does not guarantee that a particular vMotion migration will be successful.

Hosts marked with a red **X** are unsuitable candidates for migration. A lack of edges connecting that host and the virtual machine's networks and datastores indicate that the host is unsuitable because of networking or datastore incompatibility. If the unsuitability is because of CPU or software incompatibility, the information appears in a tooltip when the pointer hovers over the host in question.

It might take a few seconds for the map to retrieve load, CPU, and software information. The state of the map's information retrieval process appears in the lower-left corner of the map. As information arrives, the map is updated. A host that looks like a good vMotion candidate (displayed as green) might become a bad candidate (displayed as red) as information is collected.

vCenter Map Icons and Interface Controls

Resource maps are visual representations of your datacenter topology. Each icon in a resource map represents a managed object or its current state. Controls in the **Maps** tab enable you to work with the current resource map.

Map Icons

The icons in a resource map represent the objects in the inventory and their current state. Table 19-1 describes the map icons.

Table 19-1. Resource Map Icons

Icon	Description
	Host icon.
	A host that is compatible for vMotion migration. The color of the circle varies in intensity based on the load of the current host. Heavily used hosts are pale; low-load hosts are saturated green.
	A host that is not compatible for vMotion migration.
	Virtual machine icon. When the virtual machine is powered on, the icon contains a green triangle.
	Network icon.
	Datastore icon.

Map Interface Controls

Use the controls in the Maps tab to customize map relationships, refresh map views, and move the focus of the current map. Table 19-2 describes the controls located on the **Maps** tab.

Table 19-2. Resource Map Interface Controls

Map Interface Panel	Description
Overview panel	Thumbnail graphic of the full-scale map.
Map Relationships panel	Displayed when more than one map view is available. The Map Relationships panel lets you customize map relationships for hosts and virtual machines. Use the checkboxes to enable or disable relationships for the selected object and display them in the current resource map.
Refresh link	Maps do not auto-refresh. Click **Refresh** to synchronize your map with the current state of the inventory and to center the map view.
Inventory panel	When selecting through the Inventory navigation bar, a selected item stays highlighted to indicate map focus. When selecting through the Maps navigation bar, all items in the inventory are listed with a check box. You can select or deselect any inventory items you do not want included in the map.

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**.

Appendixes

Defined Privileges

A

The following tables list the default privileges that, when selected for a role, can be paired with a user and assigned to an object. The tables in this appendix use VC to indicate vCenter Server and HC to indicate host client, a standalone ESX/ESXi host.

When setting permissions, verify all the object types are set with appropriate privileges for each particular action. Some operations require access permission at the root folder or parent folder in addition to access to the object being manipulated. Some operations require access or performance permission at a parent folder and a related object.

vCenter Server extensions might define additional privileges not listed here. Refer to the documentation for the extension for more information on those privileges.

This appendix includes the following topics:

Alarms

Alarms privileges control the ability to set and respond to alarms on inventory objects.

Table A-1 describes privileges needed to create, modify, and respond to alarms.

Table A-1. Alarms Privileges

Privilege Name	Description	Used	Pair with Object	Effective on Object
Acknowledge alarm	Suppresses all alarm actions from occurring on all triggered alarms. User interface element – **Triggered Alarms** panel	VC only	All inventory objects	Object on which an alarm is defined
Create alarm	Creates a new alarm. When creating alarms with a custom action, privilege to perform the action is verified when the user creates the alarm. User interface element– **Alarms** tab context menu, **File > New > Alarm**	VC only	All inventory objects	Object on which an alarm is defined
Disable alarm action	Stops the alarm action from occurring after an alarm has been triggered. This does not disable the alarm from triggering. User interface element – **Inventory > object_name > Alarm > Disable All Alarm Actions**	VC only	All inventory objects	Object on which an alarm is defined
Modify alarm	Changes the properties of an existing alarm. User interface element – **Alarms** tab context menu	VC only	All inventory objects	Object on which an alarm is defined
Remove alarm	Deletes an existing alarm. User interface element – **Alarms** tab context menu	VC only	All inventory objects	Object on which an alarm is defined
Set alarm status	Changes the status of the configured event alarm. The status can change to **Normal**, **Warning**, or **Alert**. User interface element – **Alarm Settings**dialog box, **Triggers** tab	VC only	All inventory objects	Object on which an alarm is defined

Datacenter

Datacenter privileges control the ability to create and edit datacenters in the vSphere Client inventory.

Table A-2 describes the privileges required to create and edit datacenters.

Table A-2. Datacenter Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create datacenter	Creates a new datacenter. User interface element– **Inventory** context menu, toolbar button, and **File > New Datacenter**	VC only	Datacenter folders or root object	Datacenter folder or root object
IP pool configuration	Allows configuration of a pool of IP addresses.	VC only	Datacenters, Datacenter folders, or root object	Datacenter
Move datacenter	Moves a datacenter. Privilege must be present at both the source and destination. User interface element – Inventory drag-and-drop	VC only	Datacenters, Datacenter folders, or root object	Datacenter, source and destination
Remove datacenter	Removes a datacenter. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element– **Inventory** context menu, **Inventory > Datacenter > Remove**, **Edit > Remove**	VC only	Datacenters, Datacenter folders, or root object	Datacenter plus parent object
Rename datacenter	Changes the name of a datacenter. User interface element – Inventory object, **Inventory** context menu, **Edit > Rename**, **Inventory > Datacenter > Rename**	VC only	Datacenters, Datacenter folders, or root object	Datacenter

Datastore

Datastore privileges control the ability to browse, manage, and allocate space on datastores.

Table A-3 describes the privileges required to work with datastores.

Table A-3. Datastore Privileges

Privilege Name	Description	Affects	Effective on Object	Pair with Object
Allocate space	Allocates space on a datastore for a virtual machine, snapshot, clone, or virtual disk.	HC and VC	Datastores	Datastores, Datastore folders
Browse datastore	Browses files on a datastore. User interface element – Add existing disk, browse for CD-ROM or Floppy media, serial or parallel port files	HC and VC	Datastores	Datastores, Datastore folders
Configure datastore	Configures a datastore.	HC and VC	Datastores	Datastores, Datastore folders
Low level file operations	Carries out read, write, delete, and rename operations in the datastore browser.	HC and VC	Datastores	Datastores, Datastore folders

Table A-3. Datastore Privileges (Continued)

Privilege Name	Description	Affects	Effective on Object	Pair with Object
Move datastore	Moves a datastore between folders. Privileges must be present at both the source and destination. User interface element – Inventory drag-and-drop	VC only	Datastore, source and destination	Datastores, Datastore folders
Remove datastore	Removes a datastore. This privilege is deprecated. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element– Inventory datastore context menu, **Inventory > Datastore > Remove**	HC and VC	Datastores	Datastores, Datastore folders
Remove file	Deletes a file in the datastore. This privilege is deprecated. Assign the **Low level file operations** User interface element – Datastore Browser toolbar button and Datastore context menu	HC and VC	Datastores	Datastores, Datastore folders
Rename datastore	Renames a datastore. User interface element– Datastore Properties dialog Change button, host Summary tab context menu	HC and VC	Datastores	Datastores, Datastore folders
Update virtual machine files	Updates file paths to virtual machine files on a datastore after the datastore has been resignatured.	HC and VC	Datastores	Datastores, Datastore folders

Distributed Virtual Port Group

Distributed virtual port group privileges control the ability to create, delete, and modify distributed virtual port groups.

Table A-4 describes the privileges required to create and configure distributed virtual port groups.

Table A-4. Distributed Virtual Port Group Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create	Create a distributed virtual port group.	HC and VC	Datacenter, Network folder	vNetwork Distributed Switch
Delete	Delete a distributed virtual port group. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Modify	Modify the configuration of a distributed virtual port group.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch

Table A-4. Distributed Virtual Port Group Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Policy operation	Set the policy of a distributed virtual port group.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Scope operation	Set the scope of a distributed virtual port group.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch

Extension

Extension privileges control the ability to install and manage extensions.

Table A-5 describes privileges required to install and manage plug-ins.

Table A-5. Extension Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Register extension	Registers an extension (plug-in)	VC only	Root vCenter Server	Root vCenter Server
Unregister extension	Unregisters an extension (plug-in)	VC only	Root vCenter Server	Root vCenter Server
Update extension	Updates an extension (plug-in)	VC only	Root vCenter Server	Root vCenter Server

Folder

Folder privileges control the abililty to create and manage folders.

Table A-6 describes privileges required to create and manage folders.

Table A-6. Folder Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create folder	Creates a new folder. User interface element– Taskbar button, **File** menu, context menu	VC only	Folders	Folders
Delete folder	Deletes a folder. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element– **File** menu, context menu	VC only	Folders plus parent object	Folders
Move folder	Moves a folder. Privilege must be present at both the source and destination. User interface element – Inventory drag-and-drop	VC only	Folders, source and destination	Folders
Rename folder	Changes the name of a folder. User interface element – Inventory pane object text field, context menu, **File** menu	VC only	Folders	Folders

Global

Global privileges control global tasks related to tasks, scripts, and extensions.

Table A-7 describes privileges required for global tasks in the vSphere Client.

Table A-7. Global Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Act as vCenter Server	Prepare or initiate a vMotion send operation or a vMotion receive operation. No user vSphere Client interface elements are associated with this privilege.	VC only	Any object	Root vCenter Server
Cancel task	Cancel a running or queued task. User interface element – Recent tasks pane context menu, **Tasks & Events** context menu. Can currently cancel clone and clone to template.	HC and VC	Any object	Inventory object related to the task
Capacity planning	Enable the use of capacity planning for planning consolidation of physical machines to virtual machines. User interface element - **Consolidation** button in toolbar.	VC only	Root vCenter Server	Root vCenter Server
Diagnostics	Get list of diagnostic files, log header, binary files, or diagnostic bundle. User interface element – **File > Export > Export Diagnostic Data**, Admin **System Logs** tab	VC only	Any object	Root vCenter Server
Disable methods	Allows servers for vCenter Server extensions to disable certain operations on objects managed by vCenter Server. No user vSphere Client interface elements are associated with this privilege.	VC only	Any object	Root vCenter Server
Enable methods	Allows servers for vCenter Server extensions to enable certain operations on objects managed by vCenter Server. No user vSphere Client interface elements are associated with this privilege.	VC only	Any object	Root vCenter Server
Global tag	Add or remove global tags.	HC and VC	Any object	Root host or vCenter Server
Health	View the health of vCenter Server components. User interface element – **vCenter Service Status** on the Home page.	VC only	Root vCenter Server	Root vCenter Server
Licenses	See what licenses are installed and add or remove licenses. User interface element – **Licenses** tab, **Configuration > Licensed Features**	HC and VC	Any object	Root host or vCenter Server
Log event	Log a user-defined event against a particular managed entity. User interface element – Should ask for a reason when shutting down or rebooting a host.	HC and VC	Any object	Any object
Manage custom attributes	Add, remove, or rename custom field definitions. User interface element – **Administration > Custom Attributes**	VC only	Any object	Root vCenter Server

Table A-7. Global Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Proxy	Allows access to an internal interface for adding or removing endpoints to or from the proxy. No user vSphere Client interface elements are associated with this privilege.	VC only	Any object	Root vCenter Server
Script action	Schedule a scripted action in conjunction with an alarm. User interface element – **Alarm Settings** dialog box	VC only	Any object	Any object
Service managers	Allows use of the resxtop command in the vSphere CLI. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Root host or vCenter Server	Root host or vCenter Server
Set custom attributes	View, create, or remove custom attributes for a managed object. User interface element – Any list view shows the fields defined and allows setting them	VC only	Any object	Any object
Settings	Read and modifie runtime VC configuration settings. User interface element – **Administration > vCenter Server Management Server Configuration**	VC only	Any object	Root vCenter Server
System tag	Add or remove system tag.	VC only	Root vCenter Server	Root vCenter Server

Host CIM

Host CIM privileges control the use of CIM for host health monitoring.

Table A-8 describes privileges used for CIM host health monitoring.

Table A-8. Host CIM Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
CIM interaction	Allow a client to obtain a ticket to use for CIM services.	HC and VC	Hosts	Hosts

Host Configuration

Host configuration privileges control the ability to configure hosts.

Table A-9 describes the privileges required to configure host settings.

Table A-9. Host Configuration Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Advanced settings	Set advanced options in host configuration. User interface element – Host **Configuration** tab > **Advanced Settings**, Inventory hierarchy context menu	HC and VC	Hosts	Hosts
Authentication Store	Configure Active Directory authentication stores. User interface element – Host **Configuration** tab > **Authentication Services**	HC and VC	Hosts	Hosts

Table A-9. Host Configuration Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Change date and time settings	Sets time and date settings on the host. User interface element – Host **Configuration** tab > **Time Configuration**	HC and VC	Hosts	Hosts
Change PciPassthru settings	Change PciPassthru settings for a host. User interface element – Host **Configuration** tab > **Advanced Settings**, Inventory hierarchy context menu	HC and VC	Hosts	Hosts
Change settings	Allows setting of lockdown mode on ESXi hosts only. User interface element – Host **Configuration** tab > **Security Profile > Lockdown Mode > Edit**	HC and VC	Hosts	Hosts (ESXi only)
Change SNMP settings	Configure, restart, and stop SNMP agent. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Hosts	Hosts
Connection	Change the connection status of a host (connected or disconnected). User interface element– Right-click Host	VC only	Hosts	Hosts
Firmware	Update the host firmware on ESXi hosts. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Hosts	Hosts (ESXi only)
Hyperthreading	Enable and disable hyperthreading in a host CPU scheduler. User interface element – Host **Configuration** tab > **Processors**	HC and VC	Hosts	Hosts
Maintenance	Put the host in and out of maintenance mode. Shut down and restart a host. User interface element– Host context menu, **Inventory > Host > Enter Maintenance Mode**	HC and VC	Hosts	Hosts
Memory configuration	Set configured service console memory reservation. This setting is applicable only on ESX hosts. User interface element – Host **Configuration** tab > **Memory**	HC and VC	Hosts	Hosts
Network configuration	Configure network, firewall, and vMotion network. User interface element – Host **Configuration** tab > **Networking**, **Network Adapter**, **DNS and Routing**	HC and VC	Hosts	Hosts
Power	Configure host power management settings. User interface element – Host **Configuration** tab > **Power Management**	HC and VC	Hosts	Hosts
Query patch	Query for installable patches and install patches on the host.	HC and VC	Hosts	Hosts
Security profile and firewall	Configure internet services, such as SSH, Telnet, SNMP, and host firewall. User interface element– Host **Configuration** tab > **Security Profile**	HC and VC	Hosts	Hosts

Table A-9. Host Configuration Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Storage partition configuration	Manages VMFS datastore and diagnostic partitions. Scan for new storage devices. Manage iSCSI. User interface element– Host **Configuration** tab > **Storage**, **Storage Adapters**, **Virtual Machine Swapfile Location**Host **Configuration** tab datastore context menu	HC and VC	Hosts	Hosts
System Management	Allows extensions to manipulate the file system on the host. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Hosts	Hosts
System resources	Update the configuration of the system resource hierarchy. User interface element – Host **Configuration** tab > **System Resource Allocation**	HC and VC	Hosts	Hosts
Virtual machine autostart configuration	Change auto-start and auto-stop order of virtual machines on a single host. User interface element– Host **Configuration** tab > **Virtual Machine Startup or Shutdown**	HC and VC	Hosts	Hosts

Host Inventory

Host inventory privileges control adding hosts to the inventory, adding hosts to clusters, and moving hosts in the inventory.

Table A-10 describes the privileges required to add and move hosts and clusters in the inventory.

Table A-10. Host Inventory Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Add host to cluster	Add a host to an existing cluster. User interface element – Inventory context menu, **File > New > Add Host**	VC only	Datacenters, Clusters, Host folders	Clusters
Add standalone host	Add a standalone host. User interface element – Toolbar button, Inventory context menu, **Inventory > Datacenter > Add Host**, **File > New > Add Host**, **Hosts** tab context menu	VC only	Datacenters, Host folders	Host folders
Create cluster	Create a new cluster. User interface elements – Toolbar button, inventory context menu, **Inventory > Datacenter > New Cluster**, **File > New > Cluster**	VC only	Datacenters, Host folders	Host folders
Modify cluster	Change the properties of a cluster. User interface element – Inventory context menu, **Inventory > Cluster > Edit Settings**, **Summary** tab	VC only	Datacenters, Host folders, Clusters	Clusters
Move cluster or standalone host	Move a cluster or standalone host between folders. Privilege must be present at both the source and destination. User interface element– Inventory hierarchy	VC only	Datacenters, Host folders, Clusters	Clusters

Table A-10. Host Inventory Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Move host	Move a set of existing hosts into or out of a cluster. Privilege must be present at both the source and destination. User interface element– Inventory hierarchy drag-and-drop	VC only	Datacenters, Host folders, Clusters	Clusters
Remove cluster	Delete a cluster or standalone host. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – Inventory context menu, **Edit > Remove**, **Inventory > Cluster > Remove**	VC only	Datacenters, Host folders, Clusters, Hosts	Clusters, Hosts
Remove host	Remove a host. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – Inventory drag-and-drop out of cluster, context menu, **Inventory > Host > Remove**	VC only	Datacenters, Host folders, Clusters, Hosts	Hosts plus parent object
Rename cluster	Rename a cluster. User interface element– Inventory single click, inventory hierarchy context menu, **Inventory > Cluster > Rename**	VC only	Datacenters, Host folders, Clusters	Clusters

Host Local Operations

Host local operations privileges control actions performed when the vSphere Client is connected directly to a host.

Table A-11 describes the privileges required for actions performed when the vSphere Client is connected directly to a single host.

Table A-11. Host Local Operations Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Add host to vCenter	Install and uninstall vCenter agents, such as vpxa and aam, on a host. No user vSphere Client interface elements are associated with this privilege.	HC only	Root host	Root host
Create virtual machine	Create a new virtual machine from scratch on a disk without registering it on the host. No user vSphere Client interface elements are associated with this privilege.	HC only	Root host	Root host
Delete virtual machine	Delete a virtual machine on disk, whether registered or not. No user vSphere Client interface elements are associated with this privilege.	HC only	Root host	Root host

Table A-11. Host Local Operations Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Manage user groups	Manage local accounts on a host. User interface element – **Users & Groups** tab (only present if the vSphere Client logs on to the host directly)	HC only	Root host	Root host
Reconfigure virtual machine	Reconfigure a virtual machine.	HC only	Root host	Root host

Host Profile

Host Profile privileges control operations related to creating and modifying host profiles.

Table A-12 describes privileges required for creating and modifying host profiles.

Table A-12. Host Profile Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Clear	Clear profile related information. Apply a profile to a host. User interface element – **Inventory > Host > Host Profile > Apply Profile**	HC and VC	Root vCenter Server	Root vCenter Server
Create	Create a host profile. User interface element – **Create Profile** button on **Profiles** tab	HC and VC	Root vCenter Server	Root vCenter Server
Delete	Delete a host profile. User interface element – **Delete host profile** button when a profile is selected	HC and VC	Root vCenter Server	Root vCenter Server
Edit	Edit a host profile. User interface element – **Edit Profile** button when a profile is selected	HC and VC	Root vCenter Server	Root vCenter Server
Export	Export a host profile User interface element - **Export Profile** link on host profile Summary tab.	HC and VC	Root vCenter Server	Root vCenter Server
View	View a host profile. User interface element – **Host Profiles** button on vSphere Client Home page	HC and VC	Root vCenter Server	Root vCenter Server

Network

Network privileges control tasks related to network management.

Table A-13 describes privileges required for network management.

Table A-13. Network Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Assign network	Assign a network to a virtual machine.	HC and VC	Networks, Network folders	Networks, Virtual Machines
Configure	Configure a network.	HC and VC	Networks, Network folders	Networks, Virtual Machines
Move network	Move a network between folders. Privilege must be present at both the source and destination. User interface element – Inventory drag-and-drop	HC and VC	Networks	Networks
Remove	Remove a network. This privilege is deprecated. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element– Inventory network context menu, **Edit > Remove**, **Inventory > Network > Remove**	HC and VC	Networks, Network folders, and Datacenters	Networks

Performance

Performance privileges control modifying performance statistics settings.

Table A-14 describes privileges required to modify performance statistics settings.

Table A-14. Performance Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Modify intervals	Creates, removes, and updates performance data collection intervals. User interface element– **Administration > vCenter Server Management Server Configuration > Statistics**	VC only	Root vCenter Server	Root vCenter Server

Permissions

Permissions privileges control the assigning of roles and permissions.

Table A-15 describes permissions required for assigning roles and permissions.

Table A-15. Permissions Privileges

Privilege Name	Description	Used	Pair with Object	Effective on Object
Modify permission	Define one or more permission rules on an entity, or updates rules if already present for the given user or group on the entity. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – **Permissions** tab context menu, **Inventory > Permissions** menu	HC and VC	All inventory objects	Any object plus parent object
Modify role	Update a role's name and its privileges. User interface element – **Roles** tab context menu, toolbar button, **File** menu	HC and VC	Root vCenter Server	Any object
Reassign role permissions	Reassign all permissions of a role to another role. User interface element – **Delete Role** dialog box, **Reassign affected users** radio button and associated menu	HC and VC	Root vCenter Server	Any object

Resource

Resource privileges control the creation and management of resource pools, as well as the migration of virtual machines.

Table A-16 describes privileges that control resource management and virtual machine migration.

Table A-16. Resource Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Apply recommendation	Ask the server to go ahead with a suggested vMotion. User interface element – Cluster DRS tab	VC only	Datacenters, Host folders, Clusters	Clusters
Assign vApp to resource pool	Assign a vApp to a resource pool. User interface element – New vApp wizard	HC and VC	Datacenters, Host folders, Clusters, Resource pools, Hosts	Resource pools
Assign virtual machine to resource pool	Assign a virtual machine to a resource pool. User interface element – New Virtual Machine wizard	HC and VC	Datacenters, Host folders, Clusters, Resource pools, Hosts	Resource pools
Create resource pool	Create a new resource pool. User interface element – **File** menu, context menu, **Summary** tab, **Resources** tab	HC and VC	Datacenters, Host folders, Clusters, Resource pools, Hosts	Resource pools, clusters
Migrate	Migrate a virtual machine's execution to a specific resource pool or host. User interface element– Inventory context menu, Virtual Machine **Summary** tab, **Inventory > Virtual Machine > Migrate**, drag-and- drop	VC only	Datacenters, Virtual machine folders, Virtual machines	Virtual machines

Table A-16. Resource Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Modify resource pool	Change the allocations of a resource pool. User interface element – **Inventory > Resource Pool > Remove**, **Resources** tab	HC and VC	Resource pools plus parent object	Resource pools
Move resource pool	Move a resource pool. Privilege must be present at both the source and destination. User interface element – Drag-and-drop	HC and VC	Resource pools, source and destination	Resource pools
Query vMotion	Query the general vMotion compatibility of a virtual machine with a set of hosts. User interface element – Required when displaying the migration wizard for a powered-on VM, to check compatibility	VC only	Root folder	Root folder
Relocate	Cold migrate a virtual machine's execution to a specific resource pool or host. User interface element– Inventory context menu, Virtual Machine **Summary** tab, **Inventory > Virtual Machine > Migrate**, drag-and- drop	VC only	Virtual machines	Virtual machines
Remove resource pool	Delete a resource pool. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – **Edit > Remove**, **Inventory > Resource Pool > Remove**, inventory context menu, **Resources** tab	HC and VC	Resource pools plus parent object	Resource pools
Rename resource pool	Rename a resource pool. User interface element – **Edit > Rename**, **Inventory > Resource Pool > Rename**, context menu	HC and VC	Resource pools	Resource pools

Scheduled Task

Scheduled task privileges control creation, editing, and removal of scheduled tasks.

Table A-17 describes privileges required for creating and modifying scheduled tasks.

Table A-17. Scheduled Task Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create tasks	Schedule a task. Required in addition to the privileges to perform the scheduled action at the time of scheduling. User interface element – **Scheduled Tasks** toolbar button and context menu	VC only	Any object	Any object
Modify task	Reconfigure the scheduled task properties. User interface element – **Inventory > Scheduled Tasks > Edit**, **Scheduled Tasks** tab context menu	VC only	Any object	Any object
Remove task	Remove a scheduled task from the queue. User interface element – **Scheduled Tasks** context menu, **Inventory > Scheduled Task > Remove**, **Edit > Remove**	VC only	Any object	Any object
Run task	Run the scheduled task immediately. Creating and running a task also requires permission to perform the associated action. User interface element – **Scheduled Tasks** context menu, **Inventory > Scheduled Task > Run**	VC only	Any object	Any object

Sessions

Sessions privileges control the ability of extensions to open sessions on the vCenter Server.

Table A-18 describes the privileges required to open sessions on vCenter Server.

Table A-18. Session Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Impersonate user	Impersonate another user. This capability is used by extensions.	VC only	Root vCenter Server	Root vCenter Server
Message	Set the global log in message. User interface element – **Sessions** tab, **Administration > Edit Message of the Day**	VC only	Root vCenter Server	Root vCenter Server
Validate session	Verifies session validity.	VC only	Root vCenter Server	Root vCenter Server
View and stop sessions	View sessions. Force log out of one or more logged-on users. User interface element– **Sessions** tab	VC only	Root vCenter Server	Root vCenter Server

Storage Views

Storage Views privileges control the ability to configure and use storage views on vCenter Server.

Table A-19 describes privileges required to configure and use storage views.

Table A-19. Storage Views Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Configure service	Allows changing options such as the reports update interval and database connectivity information.	VC only	Root vCenter Server	Root vCenter Server
View	View Storage Views tab. User interface element – **Storage Views** tab.	VC only	Root vCenter Server	Root vCenter Server

Tasks

Tasks privileges control the ability of extensions to create and update tasks on the vCenter Server.

Table A-20 describes privileges related to tasks.

Table A-20. Tasks Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create task	Allows an extension to create a user-defined task.	VC only	Root vCenter Server	Root vCenter Server
Update task	Allows an extension to updates a user-defined task.	VC only	Root vCenter Server	Root vCenter Server

vApp

vApp privileges control operations related to deploying and configuring a vApp.

Table A-21 describes privileges related to vApps.

Table A-21. vApp Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Add virtual machine	Add a virtual machine to a vApp. User interface element – drag-and-drop in the Virtual Machines and Templates or Hosts and Clusters inventory view	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Assign resource pool	Assign a resource pool to a vApp. User interface element – drag-and-drop in the Hosts and Clusters inventory view	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Assign vApp	Assign a vApp to another vApp User interface element – drag-and-drop in the Virtual Machines and Templates or Hosts and Clusters inventory view	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Clone	Clone a vApp. User interface element – **Inventory > vApp > Clone**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Create	Create a vApp.	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps

Table A-21. vApp Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Delete	Delete a vApp. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – **Inventory > vApp > Delete from Disk**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Export	Export a vApp from vSphere. User interface element – **File > Export > Export OVF Template**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Import	Import a vApp into vSphere. User interface element – **File > Deploy OVF Template**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Move	Move a vApp to a new inventory location. User interface element – drag-and-drop in the Virtual Machines and Templates or Hosts and Clusters inventory view	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Power Off	Power off a vApp. User interface element – **Inventory > vApp > Power Off**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Power On	Power on a vApp. User interface element – **Inventory > vApp > Power On**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Rename	Rename a vApp. User interface element – **Inventory > vApp > Rename**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Suspend	Suspend a vApp. User interface element – **Inventory > vApp > Suspend**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
Unregister	Unregister a vApp. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – **Inventory > vApp > Remove from Inventory**	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
vApp application configuration	Modify a vApp's internal structure, such as product information and properties. User interface element – Edit vApp Settings dialog box, **Options** tab, **Advanced** option	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
vApp instance configuration	Modify a vApp's instance configuration, such as policies. User interface element – Edit vApp Settings dialog box, **Options** tab, **Properties** option and **IP Allocation Policy** option	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps

Table A-21. vApp Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
vApp resource configuration	Modify a vApp's resource configuration. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – Edit vApp Settings dialog box, **Options** tab, **Resources** option	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps
View OVF Environment	View the OVF environment of a powered-on virtual machine within a vApp. User interface element – Virtual Machine Properties dialog box, **Options** tab, **OVF Settings** option, **View** button	VC only	Datacenters, clusters, hosts, virtual machine folders, vApps	vApps

Virtual Machine Configuration

Virtual Machine Configuration privileges control the ability to configure virtual machine options and devices.

Table A-22 describes privileges required for configuring virtual machine options and devices.

Table A-22. Virtual Machine Configuration Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Add existing disk	Add an existing virtual disk to a virtual machine. User interface element – Virtual Machine Properties dialog box	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Add new disk	Create a new virtual disk to add to a virtual machine. User interface element – Virtual Machine Properties dialog box	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Add or remove device	Add or removes any non-disk device. User interface element – Virtual Machine Properties dialog box	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Advanced	Add or modify advanced parameters in the virtual machine's configuration file. User interface element – Virtual Machine Properties dialog box > **Options** tab > **Advanced** - **General** option > **Configuration Parameters** button	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-22. Virtual Machine Configuration Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Change CPU count	Change the number of virtual CPUs. User interface element – Virtual Machine Properties dialog box	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Change resource	Change resource configuration of a set of VM nodes in a given resource pool.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Disk change tracking	Enable or disable change tracking for the virtual machine's disks.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Disk lease	Leases disks for VMware Consolidated Backup. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Extend virtual disk	Expand the size of a virtual disk.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Host USB device	Attach a host-based USB device to a virtual machine.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Memory	Change the amount of memory allocated to the virtual machine. User interface element – Virtual Machine Properties dialog box > **Memory**	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Modify device settings	Change the properties of an existing device. User interface element – Virtual Machine Properties dialog box > SCSI/IDE node selection	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-22. Virtual Machine Configuration Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Query Fault Tolerance compatibility	Check if a virtual machine is compatible for Fault Tolerance.	VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Query unowned files	Query unowned files.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Raw device	Add or removes a raw disk mapping or SCSI pass through device. Setting this parameter overrides any other privilege for modifying raw devices, including connection states. User interface element – Virtual Machine Properties > Add/Remove raw disk mapping	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Reload from path	Change a virtual machine configuration path while preserving the identity of the virtual machine. Solutions such as VMware vCenter Site Recovery Manager use this operation to maintain virtual machine identity during failover and failback. No user vSphere Client interface elements are associated with this privilege.	VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Remove disk	Remove a virtual disk device. User interface element – Virtual Machine Properties dialog box > Hard Disk (but not a raw disk mapping)	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Rename	Rename a virtual machine or modifies the associated notes of a virtual machine. User interface element– Virtual Machine Properties dialog box, inventory, inventory context menu, **File** menu, **Inventory** menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Reset guest information	Edit the guest operating system information for a virtual machine User interface element – Virtual Machine Properties dialog box **Options** tab,	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Settings	Change general VM settings. User interface element – Virtual Machine Properties dialog box **Options** tab, **General Options** option	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-22. Virtual Machine Configuration Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Swapfile placement	Change the swapfile placement policy for a virtual machine. User interface element – Virtual Machine Properties dialog box **Options** tab, **Swapfile Location** option	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Unlock	Allow decrypting a virtual machine.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Upgrade virtual hardware	Upgrade the virtual machine's virtual hardware version from a previous version of VMware. User interface element – context menu, **File** menu (appears only if vmx file shows a lower configuration number)	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Virtual Machine Interaction

Virtual Machine Interaction privileges control the ability to interact with a virtual machine console, configure media, perform power operations, and install VMware Tools.

Table A-23 describes privileges required for virtual machine interaction.

Table A-23. Virtual Machine Interaction

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Acquire guest control ticket	Acquire a ticket to connect to a virtual machine guest control service remotely.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Answer question	Resolve issues with VM state transitions or runtime errors. User interface element – **Summary** tab, Inventory menu, context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Backup operation on virtual machine	Perform backup operations on virtual machines.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-23. Virtual Machine Interaction (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Configure CD media	Configure a virtual DVD or CD-ROM device. User interface element – Virtual Machine Properties dialog box > DVD/CD-ROM	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Configure floppy media	Configure a virtual floppy device. User interface element – Virtual Machine Properties dialog box, **Summary** tab **Edit Settings**	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Console interaction	Interact with the virtual machine's virtual mouse, keyboard, and screen. User interface element– **Console** tab, toolbar button, **Inventory > Virtual Machine > Open Console**, inventory context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Create screenshot	Create a virtual machine screen shot.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Defragment all disks	Defragment all disks on the virtual machine.	HC and VC.	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Device connection	Change the connected state of a virtual machine's disconnectable virtual devices. User interface element– Virtual Machine Properties dialog box, **Summary** tab **Edit Settings**	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Disable Fault Tolerance	Disable the Secondary virtual machine for a virtual machine using Fault Tolerance. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Disable Fault Tolerance**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Enable Fault Tolerance	Enable the Secondary virtual machine for a virtual machine using Fault Tolerance. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Enable Fault Tolerance**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-23. Virtual Machine Interaction (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Power Off	Power off a powered-on virtual machine, shuts down guest. User interface element – **Inventory > Virtual Machine > Power > Power Off**, **Summary** tab, toolbar button, virtual machine context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Power On	Power on a powered-off virtual machine, resumes a suspended virtual machine. User interface element– **Inventory > Virtual Machine > Power > Power On**, **Summary** tab, toolbar button, virtual machine context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Record session on Virtual Machine	Record a session on a virtual machine. No vSphere Client user interface elements are associated with this privilege.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Replay session on Virtual Machine	Replay a recorded session on a virtual machine. No vSphere Client user interface elements are associated with this privilege.	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Reset	Resets virtual machine and reboots the guest operating system. User interface element – **Inventory > Virtual Machine > Power > Reset**, **Summary** tab, toolbar button, virtual machine context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Suspend	Suspends a powered-on virtual machine, puts guest in standby mode. User interface element – **Inventory > Virtual Machine > Power > Suspend**, **Summary** tab, toolbar button, virtual machine context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Test failover	Test Fault Tolerance failover by making the Secondary virtual machine the Primary virtual machine. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Test Failover**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Test restart Secondary VM	Terminate a Secondary virtual machine for a virtual machine using Fault Tolerance. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Test Restart Secondary**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Table A-23. Virtual Machine Interaction (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Turn Off Fault Tolerance	Turn off Fault Tolerance for a virtual machine. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Turn Off Fault Tolerance**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
Turn On Fault Tolerance	Turn on Fault Tolerance for a virtual machine. User interface element – **Inventory > Virtual Machine > Fault Tolerance > Turn On Fault Tolerance**	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines
VMware Tools install	Mounts and unmounts the VMware Tools CD installer as a CD-ROM for the guest operating system. User interface element– **Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**,virtual machine context menu	HC and VC	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Virtual Machine Inventory

Virtual Machine Inventory privileges control adding, moving, and removing virtual machines.

Table A-24 describes privileges required to add, move, and remove virtual machines in the inventory.

Table A-24. Virtual Machine Inventory Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create from existing	Create a virtual machine based on an existing virtual machine or template, by cloning or deploying from a template.	HC and VC	Datacenters, Clusters, Hosts, Virtual machine folders	Clusters, Hosts, Virtual machine folders
Create new	Create a new virtual machine and allocates resources for its execution. User interface element– **File** menu, context menu, **Summary** tab - **New Virtual Machine** links	HC and VC	Datacenters, Clusters, Hosts, Virtual machine folders	Clusters, Hosts, Virtual machine folders
Move	Relocate a virtual machine in the hierarchy. Privilege must be present at both the source and destination. User interface element – Inventory hierarchy drag-and-drop in Virtual Machines & Templates view	VC only	Datacenters, Clusters, Hosts, Virtual machine folders, Virtual machines	Virtual machines
Register	Add an existing virtual machine to a vCenter Server or host inventory.	HC and VC	Datacenters, Clusters, Hosts, Virtual machine folders	Clusters, Hosts, Virtual machine folders

Table A-24. Virtual Machine Inventory Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Remove	Delete a virtual machine, removing its underlying files from disk. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object. User interface element – **File** menu, context menu, **Summary** tab	HC and VC	Datacenters, Clusters, Hosts, Virtual machine folders, Virtual machines	Virtual machines
Unregister	Unregister a virtual machine from a vCenter Server or host inventory. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	HC and VC	Datacenters, Clusters, Hosts, Virtual machines, virtual machine folders	Virtual machines

Virtual Machine Provisioning

Virtual Machine Provisioning privileges control activities related to deploying and customizing virtual machines.

Table A-25 describes privileges required for virtual machine provisioning.

Table A-25. Virtual Machine Provisioning Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Allow disk access	Open a disk on a virtual machine for random read and write access. Used mostly for remote disk mounting. No user vSphere Client interface elements are associated with this privilege.	n/a	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Allow read-only disk access	Open a disk on a virtual machine for random read access. Used mostly for remote disk mounting. No user vSphere Client interface elements are associated with this privilege.	n/a	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Allow virtual machine download	Read files associated with a virtual machine, including vmx, disks, logs, and nvram. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Root folders

Table A-25. Virtual Machine Provisioning Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Allow virtual machine files upload	Write files associated with a virtual machine, including vmx, disks, logs, and nvram. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Root folders
Clone template	Clone a template. User interface element– **Inventory > Virtual Machine > Template > Clone**, context menu, **Virtual Machines** tab	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Templates	Templates
Clone virtual machine	Clone an existing virtual machine and allocates resources. User interface element – **Inventory > Virtual Machine > Clone**, context menu, **Summary** tab	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Create template from virtual machine	Create a new template from a virtual machine. User interface element – **Inventory > Virtual Machine > Template > Clone to Template**, context menu, **Summary** tab items	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Customize	Customize a virtual machine's guest operating system without moving the virtual machine. User interface element– Clone Virtual Machine wizard: Guest Customization	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Deploy template	Deploy a virtual machine from a template. User interface element – "Deploy to template" **File** menu, context menu items, **Virtual Machines** tab	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Templates	Templates
Mark as template	Mark an existing, powered off virtual machine as a template. User interface element – **Inventory > Virtual Machine > Template > Convert to Template**, context menu items, **Virtual Machines** tab, **Summary** tab	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines

Table A-25. Virtual Machine Provisioning Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Mark as virtual machine	Mark an existing template as a VM. User interface element – "Convert to Virtual Machine..." context menu items, **Virtual Machines** tab	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Templates	Templates
Modify customization specification	Create, modify, or delete customization specifications. User interface element – Customization Specifications Manager	VC only	Root vCenter Server	Root vCenter Server
Promote disks	Promote a virtual machine's disks.	VC only	Datacenters, Hosts, Clusters, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Read customization specifications	Read a customization specification	VC only	Datacenters, Hosts, Clusters, Virtual machine folders, Resource pools, Virtual machines	Virtual machines

Virtual Machine State

Virtual machine state privileges control the ability to take, delete, rename, and restore snapshots.

Table A-26 describes privileges required to work with virtual machine snapshots.

Table A-26. Virtual Machine State Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create snapshot	Create a new snapshot from the virtual machine's current state. User interface element – virtual machine context menu, toolbar button, **Inventory > Virtual Machine > Snapshot > Take Snapshot**	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Remove Snapshot	Remove a snapshot from the snapshot history. User interface element – virtual machine context menu, toolbar button, **Inventory** menu	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines

Table A-26. Virtual Machine State Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Rename Snapshot	Rename this snapshot with either a new name or a new description or both. No user vSphere Client interface elements are associated with this privilege.	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Revert to snapshot	Set the VM to the state it was in at a given snapshot. User interface element – virtual machine context menu, toolbar button, **Inventory > Virtual Machine > Snapshot > Revert to Snapshot**, **Virtual Machines** tab	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines

vNetwork Distributed Switch

vNetwork Distributed Switch privileges control the ability to perform tasks related to the management of vNetwork Distributed Switches.

Table A-27 describes the privileges required to create and configure vNetwork Distributed Switches.

Table A-27. vNetwork Distributed Switch Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Create	Create a vNetwork Distributed Switch.	HC and VC	Datacenter, Network folder	Datacenter, Network folder
Delete	Remove a vNetwork Distributed Switch. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Host operation	Change the host members of a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Modify	Change the Configuration of a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Move	Move a vNetwork Distributed Switch into another folder.	VC only	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Network resource managment operation	Change the resource settings for a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Policy operation	Change the policy of a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch

Table A-27. vNetwork Distributed Switch Privileges (Continued)

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Port configuration operation	Change the configuration of a port in a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
Port setting operation	Change the setting of a port in a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch
VSPAN operation	Change the VSPAN configuration of a vNetwork Distributed Switch.	HC and VC	vNetwork Distributed Switch, Network folder, Datacenter	vNetwork Distributed Switch

VRM Policy

VRM policy privileges control the ability to query and update virtual rights management policies.

Table A-28 describes privileges related to virtual rights management.

Table A-28. VRM Policy Privileges

Privilege Name	Description	Affects	Pair with Object	Effective on Object
Query VRMPolicy	Query virtual rights management policy.	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines
Update VRMPolicy	Update virtual rights management policy.	HC and VC	Datacenters, Clusters, Hosts, Resource pools, Virtual machine folders, Virtual machines	Virtual machines

Performance Metrics

B

vSphere collects performance data on managed objects. Performance metrics organize this data into the following categories:

Table B-1. Metric Groups

Metric group	Description
Cluster Services	Performance statistics for clusters configured by using VMware DRS (distributed resource scheduler), VMware HA (high availability), or both.
CPU	CPU utilization per host, virtual machine, resource pool, or compute resource.
Datastore	Statistics for datastore utilization
Disk	Disk utilization per host, virtual machine, or datastore. Disk metrics include I/O performance (such as latency and read/write speeds), and utilization metrics for storage as a finite resource.
Management Agent	Memory swap statistics per COS.
Memory	Memory utilization per host, virtual machine, resource pool, or compute resource. The value obtained is one of the following: ■ For virtual machines, memory refers to guest physical memory. Guest physical memory is the amount of physical memory presented as a virtual-hardware component to the virtual machine, at creation time, and made available when the virtual machine is running. ■ For hosts, memory refers to machine memory. Machine memory is the RAM that is installed in the hardware that comprises the ESX/ESXi system.
Network	Network utilization for both physical and virtual network interface controllers (NICs) and other network devices, such as the virtual switches (vSwitch) that support connectivity among all components (hosts, virtual machines, VMkernel, and so on).
Power	Energy usage statistics per host.
Storage Adapter	Data traffic statistics per HBA.
Storage Path	Data traffic statistics per path.
System	Overall system availability, such as system heartbeat and uptime. These counters are available directly from ESX and from vCenter Server.
Virtual Machine Operations	Virtual machine power and provisioning operations in a cluster or datacenter.

Each metric group contains one or more data counters (Appendix C, "Data Counters," on page 269). vCenter Server collects and stores data for all counters. However, the counters that are available for customizing a performance chart depend on the Statistics Level setting ("Statistics Levels," on page 114, and the selected time period (Real Time, Past Day, and so on).

Calculations for all metrics are for the duration of the data collection cycle. Collection cycle durations are specified by the Statistics Interval > Interval Duration setting.

You can use the vShpere Web Services SDK to query vCenter Server and get statistics for all counters. The *VMware vSphere API Reference* contains detailed information about all data counters.

Data Counters

C

vCenter Server systems and ESX/ESXi hosts use data counters to query for statistics. A data counter is a unit of information relevant to a given object.

For example, network metrics for a virtual machine include one counter that tracks the rate at which data is transmitted and another counter that tracks the rate at which data is received across a NIC instance.

Each data counter is comprised of several attributes that are used to determine the statistical value collected. Table C-1 lists the data counter attributes.

Table C-1. Data Counter Attributes

Attribute	Description
Unit of measurement	How the statistic quantity is measured. ■ KiloBytes (KB) – 1024 bytes ■ KiloBytes per second (KBps) – 1024 bytes per second ■ Kilobits (kb) – 1000 bits ■ Kilobits per second (kbps) – 1000 bits per second ■ MegaBytes (MB) ■ MegaBytes per second (MBps) ■ Megabits (mb) ■ Megabits per second (mbps) ■ MegaHertz (MHz) ■ Microseconds (µs) ■ Milliseconds (ms) ■ Number (#) ■ Percentage (%) ■ Seconds (s)
Description	Text description of the data counter.
Statistics type	Measurement used during the statistics interval. Related to the unit of measurement. ■ Rate – Value over the current statistics interval ■ Delta – Change from previous statistics interval ■ Absolute – Absolute value, independent of the statistics interval

Table C-1. Data Counter Attributes (Continued)

Attribute	Description
Rollup Type	Calculation method used during the statistics interval to roll up data. This determines the type of statistical values that are returned for the counter. One of: ■ Average – Data collected during the interval is aggregated and averaged. ■ Minimum – The minimum value is rolled up. ■ Maximum – The maximum value is rolled up. The Minimum and Maximum values are collected and displayed only in collection level 4. Minimum and maximum rollup types are used to capture peaks in data during the interval. For real-time data, the value is the current minimum or current maximum. For historical data, the value is the average minimum or average maximum. Minimum and maximum rollup types are denoted in the collection level value by parentheses. For example, the following information for the CPU usage chart shows that the average value is calculated and displayed at collection level 1 and the minimum and maximum values are displayed at collection level 4. ■ Counter: usage ■ Stats Type: Rate ■ Unit: Percentage (%) ■ Rollup Type: Average (Minimum/Maximum) ■ Collection Level: 1 (4) ■ Summation – Data collected is summed. The measurement displayed in the chart represents the sum of data collected during the interval. ■ Latest – Data collected during the interval is a set value. The value displayed in the performance charts represents the current value.
Collection level	Number of data counters used to collect statistics. Collection levels range from 1 to 4, with 4 having the most counters.

Index

D

Q

R

S

T

U

V

W