VMware vSphere Examples and Scenarios

Update 1
vSphere 5.0
vCenter Server 5.0
ESXi 5.0

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

EN-000833-00

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

About vSphere Examples and Scenarios

1

The examples and scenarios in this publication identify tasks in vSphere and suggest ways to accomplish them.

For instance, for the first-time user who wants to evaluate vCenter Server, *vSphere Examples and Scenarios* contains Chapter 2, "Getting Started with ESXi," on page 7 and Chapter 3, "Getting Started with vCenter Server," on page 19. These sections guide the user through tasks that result in having a virtual machine on an ESXi host, both of which are managed with vCenter Server through the vSphere Client.

In a different scenario, someone who wants to see how vSphere can be configured to send email notifications when alarm threshholds are crossed can review Chapter 10, "Alarm Example: Setting an Alarm Action for Datastore Usage on a Disk," on page 91. Other scenarios deal with networking, virtual machine deployment, and so on.

Everyone's environment and policy set is different. VMware recommends that you first experiment with the procedures presented in *vSphere Examples and Scenarios* on test instances in your datacenter.

This document is not for troubleshooting. For problems that you might be experiencing, see *vSphere Troubleshooting*.

Getting Started with ESXi 2

Get started with ESXi quickly with information about installation and initial setup. The procedures show you how to install and set up a basic inventory for a single-host virtualization environment.

This information is for experienced Windows or Linux system administrators who will be installing VMware ESXi to deploy virtualization for the first time. Specifically, it is for users who meet the following requirements:

- Do not yet have the ESXi software installed
- Do not yet have the vSphere Client or VMware vCenter Server installed

After your host is set up, but before you install a working virtual machine, you can install vCenter Server and explore a multiple-host virtualization environment. See "Getting Started Workflows for Single-Host or Multiple-Host Systems," on page 7.

This chapter includes the following topics:

Getting Started Workflows for Single-Host or Multiple-Host Systems

The getting started tasks take you from initial setup of a new virtualization host to a working virtual machine.

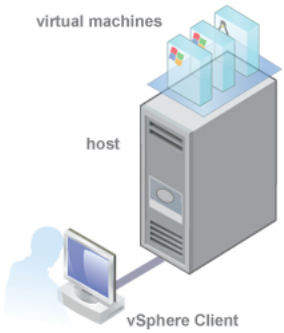
Getting Started Tasks for a Basic Single-Host Management System

Getting started with ESXi includes the following tasks:

- Install ESXi and add the host to your network
- Install the vSphere Client and connect to the ESXi host
- Deploy and run a virtual machine

The getting started tasks set up the single-host management system for virtualization.

Figure 2-1. Basic Single-Host Management System



After the initial setup of ESXi, you can deploy vSphere with vCenter Server to manage multiple hosts.

Getting Started Tasks to Evaluate vCenter Server for a Multiple-Host Management System

Getting started with ESXi and vCenter Server includes the following tasks:

- Install ESXi and add the host to your network
- Install the vSphere Client and connect to the ESXi host
- Install and set up vCenter Server by following the procedures in *Getting Started with vCenter Server*
- Deploy and run a virtual machine

ESXi Installation

Install ESXi as the first step in the process of having working virtual machines. The machine that is running ESXi virtualization software will act as a host in your virtual infrastructure.

Hosts provide CPU and memory resources, access to storage, and network connectivity for virtual machines that reside on them.

ESXi Hardware Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi 5.0.

Hardware and System Resources

To install and use ESXi 5.0, your hardware and system resources must meet the following requirements:

- Supported server platform. For a list of supported platforms, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- ESXi 5.0 will install and run only on servers with 64-bit x86 CPUs.
- ESXi 5.0 requires a host machine with at least two cores.
- ESXi 5.0 supports only LAHF and SAHF CPU instructions.
- ESXi supports a broad range of x64 multicore processors. For a complete list of supported processors, see the VMware compatibility guide at http://www.vmware.com/resources/compatibility.
- ESXi requires a minimum of 2GB of physical RAM. VMware recommends 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.

- One or more Gigabit or 10Gb Ethernet controllers. For a list of supported network adapter models, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- Any combination of one or more of the following controllers:
  - Basic SCSI controllers. Adaptec Ultra-160 or Ultra-320, LSI Logic Fusion-MPT, or most NCR/Symbios SCSI.
  - RAID controllers. Dell PERC (Adaptec RAID or LSI MegaRAID), HP Smart Array RAID, or IBM (Adaptec) ServeRAID controllers.
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks will be considered remote, not local. These disks will not be used as a scratch partition by default because they are seen as remote.

  NOTE You cannot connect a SATA CD-ROM device to a virtual machine on an ESXi 5.0 host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

ESXi 5.0 supports installing on and booting from the following storage systems:

- SATA disk drives. SATA disk drives connected behind supported SAS controllers or supported on-board SATA controllers.

  Supported SAS controllers include:
  - LSI1068E (LSISAS3442E)
  - LSI1068 (SAS 5)
  - IBM ServeRAID 8K SAS controller
  - Smart Array P400/256 controller
  - Dell PERC 5.0.1 controller

  Supported on-board SATA include:
  - Intel ICH9
  - NVIDIA MCP55
  - ServerWorks HT1000

  NOTE ESXi does not support using local, internal SATA drives on the host server to create VMFS datastores that are shared across multiple ESXi hosts.
- Serial Attached SCSI (SAS) disk drives. Supported for installing ESXi 5.0 and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI
- USB devices. Supported for installing ESXi 5.0. For a list of supported USB devices, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

ESXi Booting Requirements

vSphere 5.0 supports booting ESXi hosts from the Unified Extensible Firmware Interface (UEFI). With UEFI you can boot systems from hard drives, CD-ROM drives, or USB media. Network booting or provisioning with VMware Auto Deploy requires the legacy BIOS firmware and is not available with UEFI.

ESXi can boot from a disk larger than 2TB provided that the system firmware and the firmware on any add-in card that you are using support it. See the vendor documentation.

NOTE Changing the boot type from legacy BIOS to UEFI after you install ESXi 5.0 might cause the host to fail to boot. In this case, the host displays an error message similar to: `Not a VMware boot bank`. Changing the host boot type between legacy BIOS and UEFI is not supported after you install ESXi 5.0.

Storage Requirements for ESXi 5.0 Installation

Installing ESXi 5.0 requires a boot device that is a minimum of 1GB in size. When booting from a local disk or SAN/iSCSI LUN, a 5.2GB disk is required to allow for the creation of the VMFS volume and a 4GB scratch partition on the boot device. If a smaller disk or LUN is used, the installer will attempt to allocate a scratch region on a separate local disk. If a local disk cannot be found the scratch partition, `/scratch`, will be located on the ESXi host ramdisk, linked to `/tmp/scratch`. You can reconfigure `/scratch` to use a separate disk or LUN. For best performance and memory optimization, VMware recommends that you do not leave `/scratch` on the ESXi host ramdisk.

Due to the I/O sensitivity of USB and SD devices the installer does not create a scratch partition on these devices. As such, there is no tangible benefit to using large USB/SD devices as ESXi uses only the first 1GB. When installing on USB or SD devices, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found, `/scratch` is placed on the ramdisk. You should reconfigure `/scratch` to use a persistent datastore following the installation.

In Auto Deploy installations, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found `/scratch` is placed on ramdisk. You should reconfigure /scratch to use a persistent datastore following the installation.

For environments that boot from a SAN or use Auto Deploy, it is not necessary to allocate a separate LUN for each ESXi host. You can co-locate the scratch regions for many ESXi hosts onto a single LUN. The number of hosts assigned to any single LUN should be weighed against the LUN size and the I/O behavior of the virtual machines.

Required Information for ESXi Installation

In an interactive installation, the system prompts you for the required system information. In a scripted installation, you must supply this information in the installation script.

For future use, note the values you use during the installation. These notes are useful if you must reinstall ESXi and reenter the values that you originally chose.

Table 2-1. Required Information for ESXi Installation

Information	Required or Optional	Default	Comments
Keyboard layout	Required	U.S. English	
VLAN ID	Optional	None	Range: 0 through 4094
IP address	Optional	DHCP	You can allow DHCP to configure the network during installation. After installation, you can change the network settings.
Subnet mask	Optional	Calculated based on the IP address	
Gateway	Optional	Based on the configured IP address and subnet mask	
Primary DNS	Optional	Based on the configured IP address and subnet mask	
Secondary DNS	Optional	None	

Table 2-1. Required Information for ESXi Installation (Continued)

Information	Required or Optional	Default	Comments
Host name	Required for static IP settings	None	vSphere Clients can use either the host name or the IP address to access the ESXi host.
Install location	Required	None	Must be at least 5GB if you install the components on a single disk.
Root password	Optional	None	The root password must contain between 6 and 64 characters.

Install ESXi Interactively

You use the ESXi CD/DVD or a USB flash drive to install the ESXi software onto a SAS, SATA, SCSI hard drive, or USB drive.

ESXi Embedded must not be on the host. ESXi Installable and ESXi Embedded cannot exist on the same host.

Prerequisites

- You must have the ESXi ISO file on CD or DVD. If you do not have the installation CD/DVD, you can create one.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- Verify that a keyboard and monitor are attached to the machine on which the ESXi software will be installed.
- Consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. Note that when you disconnect network storage, any files on the disconnected disks are unavailable at installation.

  Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.
- Gather the information required by the ESXi installation wizard. See "Required Information for ESXi Installation," on page 10.

Procedure

1. Insert the ESXi CD/DVD into the CD/DVD-ROM drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device.

   See your hardware vendor documentation for information on changing boot order.
3. On the Select a Disk page, select the drive on which to install ESXi and press Enter.

   Press F1 for information about the selected disk.

   NOTE Do not rely on the disk order in the list to select a disk. The disk order is determined by the BIOS and might be out of order. This might occur on systems where drives are continuously being added and removed.

   If the disk you selected contains data, the Confirm Disk Selection page appears.
4. Select the keyboard type for the host.

   You can change the keyboard type after installation in the direct console.

5 Enter the root password for the host.

You can leave the password blank, but to secure the system from the first boot, enter a password. You can change the password after installation in the direct console.

6 Press F11 to start the installation.

7 When the installation is complete, remove the installation CD or DVD.

8 Press Enter to reboot the host.

If you are performing a new installation, or you chose to overwrite an existing VMFS datastore, during the reboot operation, VFAT scratch and VMFS partitions are created on the host disk.

9 Set the first boot device to be the drive on which you installed ESXi in Step 3.

For information about changing boot order, see your hardware vendor documentation.

What to do next

Set up basic administration and network configuration for ESXi.

Setting Up ESXi

To set up ESXi, configure the Administrative (root) password for the ESXi host and configure the default networking behavior.

You must have the following setup:

- An ESXi system that is connected to a monitor and a keyboard.
- The ESXi system is powered on.
- At least one other computer to act as a management station. This computer must be running Windows and have network access to the ESXi host. You install the vSphere Client on this machine.

Consider using a network with a DHCP server.

NOTE If a system failure occurs, you can restore the ESXi software.

After you install and boot ESXi for the first time, the system network and storage devices are configured with defaults. After the host completes the autoconfiguration phase, the direct console appears on the attached monitor.

Using a keyboard attached to the host, press F2 while in the direct console to examine the default configuration. As the system administrator, you can make changes to the default configuration, such as creating the administrator password or setting the static IP address. VMware recommends that you configure your administrative access settings and server network.

Set the Password for the Administrator Account

You can use the direct console to set the password for the administrator account (root).

The administrative user name for the ESXi host is root. By default, the administrative password is not set.

Procedure

1 From the direct console, select **Configure Password**.

2 (Optional) If a password is already set up, type the password in the **Old Password** line and press Enter.

3 In the **New Password** line, type a new password and press Enter.

4 Retype the new password and press Enter.

Configuring IP Settings for ESXi

By default, DHCP sets the IP address, subnet mask, and default gateway.

For future reference, write down the IP address.

For DHCP to work, your network environment must have a DHCP server. If DHCP is not available, the host assigns the link local IP address, which is in the subnet 169.254.x.x/16. The assigned IP address appears on the direct console. If you do not have physical monitor access to the host, you can access the direct console using a remote management application. See the *vSphere Installation and Setup* documentation.

When you have access to the direct console, you can optionally configure a static network address. The default subnet mask is 255.255.0.0.

If your network lacks a DHCP server, configure the IP settings for ESXi manually from the direct console.

Configure IP Settings from the Direct Console

If you have physical access to the host or remote access to the direct console, you can use the direct console to configure the IP address, subnet mask, and default gateway.

Procedure

1 Select **Configure Management Network** and press Enter.

2 Select **IP Configuration** and press Enter.

3 Select **Set static IP address and network configuration**.

4 Enter the IP address, subnet mask, and default gateway and press Enter.

Configure DNS Settings from the Direct Console

If you have physical access to the host or remote access to the direct console, you can use the direct console to configure DNS information.

Procedure

1 Select **Configure Management Network** and press Enter.

2 Select **DNS Configuration** and press Enter.

3 Select **Use the following DNS server addresses and hostname**.

4 Enter the primary server, an alternative server (optional), and the host name.

Managing the ESXi Host with the vSphere Client

You can manage hosts using the vSphere Client.

After you finish initial setup of the host, download and install the vSphere Client.

vSphere Client Hardware Requirements

Make sure that the vSphere Client hardware meets the minimum requirements.

vSphere Client Minimum Hardware Requirements and Recommendations

Table 2-2. vSphere Client Minimum Hardware Requirements and Recommendations

vSphere Client Hardware	Requirements and Recommendations
CPU	1 CPU
Processor	500MHz or faster Intel or AMD processor (1GHz recommended)
Memory	500MB (1GB recommended)
Disk Storage	1.5GB free disk space for a complete installation, which includes the following components: ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# Remove any previously installed versions of Microsoft Visual J# on the system where you are installing the vSphere Client. ■ vSphere Client If you do not have any of these components already installed, you must have 400MB free on the drive that has the `%temp%` directory. If you have all of the components already installed, 300MB of free space is required on the drive that has the `%temp%` directory, and 450MB is required for vSphere Client.
Networking	Gigabit connection recommended

vSphere Client and vSphere Web Client Software Requirements

Make sure that your operating system supports the vSphere Client.

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

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

The following browsers are supported for the vSphere Web Client:

- Microsoft Internet Explorer 7 and 8
- Mozilla Firefox 3.6

The vSphere Web Client requires the Adobe Flash Player version 10.1.0 or later to be installed with the appropriate plug-in for your browser.

Download the vSphere Client

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

Prerequisites

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

The system must have an Internet connection.

Procedure

1 From a Windows machine, open a Web browser.

2 Enter the URL or IP address for the vCenter Server or host.

For example, `http://exampleserver.example.com` or `http://xxx.xxx.xxx.xxx`.

3 Click **Download vSphere Client** under Getting Started.

4 Click **Save** to download the vSphere Client installer.

The vSphere Client installer is downloaded to the system.

What to do next

Install the vSphere Client.

Install the vSphere Client

The vSphere Client enables you to connect to an ESXi host and to a vCenter Server system.

The vSphere Client must be installed on a Windows machine that has network access to the ESXi host and Internet access.

When you use the vSphere Client, the vSphere Client appears in the language associated with the locale setting on the machine. You can alter this behavior with a command-line instruction or by changing the locale in the registry of the machine. See the *vCenter Server and Host Management* documentation.

Prerequisites

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

Procedure

1 Double-click the `VMware-viclient`*`build number`*`.exe` file to run the vSphere Client installer.

2 Follow the prompts in the wizard to complete the installation.

What to do next

Connect to the host with the vSphere Client.

Start the vSphere Client and Log In to ESXi

When you connect to a host with the vSphere Client, you can manage the host as well as all of the virtual machines that the host manages.

Procedure

1 Select **Start > Programs > VMware > VMware vSphere Client**.

2 Log in to the ESXi host as the root user.

   a Enter the IP address or host name.

   b Enter the username **`root`**.

   c Enter the password you set in the direct console.

3 Click **Login**.

   A security warning appears.

4 To continue, click **Ignore**.

   This security warning message occurs because the vSphere Client detected a certificate that the ESXi host signed (default setting). For highly secure environments, VMware recommends certificates that a trusted third party generates. You can set up third-party certificates later.

What to do next

- If you are performing the getting started tasks for a basic single-host management system, after you connect to the host with the vSphere Client, use the **Getting Started** tabs to import a virtual appliance.
- If you are performing the getting started tasks for evaluating vCenter Server for a multiple-host management system, do not import a virtual appliance. Install and set up vCenter Server by following the procedures in *Getting Started with vCenter Server*.

Add a Virtual Machine by Importing a Virtual Appliance

After you connect to the host machine, you can add a virtual machine to the host. You can import or create one or more virtual machines on a single host. If this is your first virtual machine, VMware recommends that you import a virtual appliance.

A virtual appliance is a prebuilt virtual machine with an operating system and applications already installed. The vSphere Client **Getting Started** tab provides steps to guide you through the options of creating a new virtual machine or importing a virtual appliance.

Procedure

1 In the **Getting Started** tab, click **Deploy from VA Marketplace**.

2 Select a virtual appliance from the list and click **Download now**.

3 Click **Next** and follow the on-screen instructions to import the virtual appliance.

You have completed setup for a single-host management system in which ESXi is used to run virtual machines.

What to do next

After you import the virtual appliance, you can use the **Console** tab in the vSphere Client to power on the virtual appliance and see what is running on it. To release the pointer from the Console, press Ctrl+Alt. To view the Console in full screen mode, from the Inventory, right-click the virtual machine and select **Open Console**.

Where to Go Next After Setting Up ESXi

You have set up your ESXi and managed it using the vSphere Client. From here, you can evaluate vCenter Server and seek information on vSphere capabilities.

- After your host is set up, you can install vCenter Server in evaluation mode and explore a multiple-host virtualization environment.

  You can manage multiple hosts at the same time with vCenter Server. Using vCenter Server to manage multiple hosts enables you to experiment with advanced management options, such as resource sharing, and all of the other options available within a virtual infrastructure.

- For more information about how to evaluate the features and benefits of vSphere, go to http://www.vmware.com/tryvmware.

The vSphere Tutorial

The vSphere tutorial contains information about many of the basic vSphere components and tasks.

You can access the tutorial through the **Explore Further** links on the **Getting Started** tabs in the vSphere Client when you want learn more about the object that you selected in the inventory.

You can also access the tutorial from the **Help** menu in the vSphere Client.

vSphere Documentation

Refer to the VMware vSphere Documentation Center for information on advanced host and vCenter Server configuration, setup for larger deployments for production environments, as well as information on advanced vSphere features.

The vSphere Documentation Center consists of the combined vCenter Server and ESXi documentation set. To access the current versions of this and other publications, go to the vSphere Documentation Center on the VMware Web site.

Getting Started with vCenter Server 3

Get started with vCenter Server quickly with information about installation and initial setup. The procedures show you how to install and set up a basic inventory for a multiple-host virtualization environment.

You can manage multiple hosts at the same time with vCenter Server. Using vCenter Server to manage multiple hosts enables you to experiment with advanced management options, such as resource sharing, and all of the other options available within a virtual infrastructure.

This publication is a continuation of the vSphere familiarization that you began in *Getting Started with ESXi*. There you set up a single-host virtualization environment, but did not create inventory objects if you knew that you were going to continue with evaluating vCenter Server.

The **Getting Started** tabs wizard appears only if there are no objects in the inventory. After you have set up the basic inventory, the **Getting Started** tabs continue to provide information about the selected inventory object but no longer provide inventory setup wizard help.

This chapter includes the following topics:

Managing Multiple Hosts with vCenter Server

Deploying vCenter Server when you deploy ESXi provides many advantages over deploying a single, standalone ESXi host.

Table 3-1. Comparison of Multiple Host Management Available with vCenter Server to Single Host Management

Feature	vCenter Server	ESXi
Scale of deployment	Multiple hosts	Single host
Capacity planning	Built in	Available separately
Server consolidation wizard	Built in	Available separately
Instant server provisioning	Available with templates and cloning	Not available
No downtime maintenance	Possible with vMotion and Storage vMotion	Not available
Load balancing	Possible with VMware DRS and Storage DRS	Not available

Table 3-1. Comparison of Multiple Host Management Available with vCenter Server to Single Host Management (Continued)

Feature	vCenter Server	ESXi
Failover	Possible with VMware HA and VMware Fault Tolerance	Not available
Power savings	Possible with VMware Distributed Power Management (DPM)	Not available
Centralized access control	Available with Active Directory Integration	Not available

vSphere and vCenter Server

VMware vSphere is a suite of virtualization applications that includes ESXi and vCenter Server.

vSphere uses virtualization to do the following tasks:

- Run multiple operating systems on a single physical machine simultaneously.
- Reclaim idle resources and balance workloads across multiple physical machines.
- Work around hardware failures and scheduled maintenance.

vSphere includes the following components in addition to the ESXi host and vSphere Client that you have already setup:

VMware vCenter Server vCenter Server unifies resources from individual hosts so that those resources can be shared among virtual machines in the entire datacenter. It accomplishes this by managing the assignment of virtual machines to the hosts and the assignment of resources to the virtual machines within a given host based on the policies that the system administrator sets.

vCenter Server allows the use of advanced vSphere features such as VMware Distributed Resource Scheduler (DRS), VMware High Availability (HA), VMware vMotion, and VMware Storage vMotion.

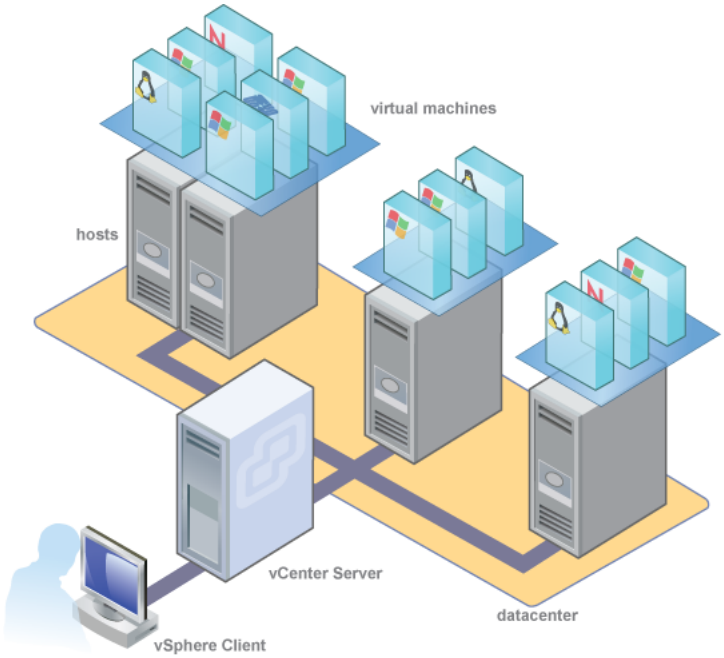
Datacenter A datacenter is a structure under which you add hosts and their associated virtual machines to the inventory.

Host A host is a computer that uses ESXi virtualization software to run virtual machines. Hosts provide CPU and memory resources, access to storage, and network connectivity for virtual machines that reside on them.

Virtual Machine A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can run on the same host at the same time. Virtual machines that vCenter Server manages can also run on a cluster of hosts.

Figure 3-1 shows the relationships among the basic components of vSphere and how vCenter Server can be used to manage hosts and run virtual machines.

Figure 3-1. vSphere Components



vCenter Server Installation

Install vCenter Server to manage multiple hosts.

To get started with vCenter Server quickly and manage the host you set up, you can install vCenter Server on a desktop or laptop. You must install vCenter Server on a Windows machine that has network access to the ESXi host. For production use, VMware recommends that you install vCenter Server on a dedicated server system.

Before you install vCenter Server, make sure your system meets the minimum hardware and software requirements. vCenter Server requires a database. vCenter Server uses Microsoft SQL Server 2008 R2 Express for small deployments with up to 5 hosts and 50 virtual machines. For larger deployments, VMware supports several Oracle and Microsoft SQL Server databases. Refer to the vSphere Compatibility Matrixes for the list of supported databases.

vCenter Server and vSphere Client Hardware Requirements

The vCenter Server system is a physical machine or virtual machine with access to a supported database. The vCenter Server system must meet specific requirements. The vCenter Server machines must meet the hardware requirements.

vCenter Server Hardware Requirements

Table 3-2. Minimum Hardware Requirements for vCenter Server

vCenter Server Hardware	Requirement
CPU	Two 64-bit CPUs or one 64-bit dual-core processor.
Processor	2.0GHz or faster Intel 64 or AMD 64 processor. The Itanium (IA64) processor is not supported. Processor requirements might be higher if the database runs on the same machine.

Table 3-2. Minimum Hardware Requirements for vCenter Server (Continued)

vCenter Server Hardware	Requirement
Memory	4GB RAM. Memory requirements might be higher if the database runs on the same machine. vCenter Server includes several Java services: VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. When you install vCenter Server, you select the size of your vCenter Server inventory to allocate memory for these services. The inventory size determines the maximum JVM heap settings for the services. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in Table 3-3.
Disk storage	4GB. Disk requirements might be higher if the vCenter Server database runs on the same machine. In vCenter Server 5.0, the default size for vCenter Server logs is 450MB larger than in vCenter Server 4.x. Make sure the disk space allotted to the log folder is sufficient for this increase.
Microsoft SQL Server 2008 R2 Express disk	Up to 2GB free disk space to decompress the installation archive. Approximately 1.5GB of these files are deleted after the installation is complete.
Networking	Gigabit connection recommended.

The recommended JVM heap settings for vCenter Server depend on your inventory size.

Table 3-3. Recommended JVM Heap Settings for vCenter Server

vCenter Server Inventory	VMware VirtualCenter Management Webservices (Tomcat)	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	1GB	2GB	512MB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	2GB	4GB	1GB
Large inventory (More than 400 hosts or 4000 virtual machines)	3GB	6GB	2GB

NOTE Installing vCenter Server on a network drive or USB flash drive is not supported.

For the hardware requirements of your database, see your database documentation. The database requirements are in addition to the vCenter Server requirements if the database and vCenter Server run on the same machine.

vSphere Client Hardware Requirements and Recommendations

Make sure that the vSphere Client host machine meets the following requirements.

Table 3-4. vSphere Client Minimum Hardware Requirements and Recommendations

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

Table 3-4. vSphere Client Minimum Hardware Requirements and Recommendations (Continued)

vSphere Client Hardware	Requirements and Recommendations
Disk Storage	1.5GB free disk space for a complete installation, which includes the following components: ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# Remove any previously installed versions of Microsoft Visual J# on the system where you are installing the vSphere Client. ■ vSphere Client If you do not have any of these components already installed, you must have 400MB free on the drive that has the `%temp%` directory. If you have all of the components already installed, 300MB of free space is required on the drive that has the `%temp%` directory, and 450MB is required for vSphere Client.
Networking	Gigabit connection recommended

vCenter Server Software Requirements

Make sure that your operating system supports vCenter Server. vCenter Server requires a 64-bit operating system, and the 64-bit system DSN is required for vCenter Server to connect to its database.

For a list of supported operating systems, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility.

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

NOTE If your vCenter Server host machine uses a non-English operating system, install both the Microsoft .NET Framework 3.5 SP1 and Microsoft .NET Framework 3.5 Language Pack through Windows Update. Windows Update automatically selects the correct localized version for your operating system. The .NET Framework installed through the vCenter Server installer includes only the English version.

If you plan to use the Microsoft SQL Server 2008 R2 Express database that is bundled with vCenter Server, Microsoft Windows Installer version 4.5 (MSI 4.5) is required on your system. You can download MSI 4.5 from the Microsoft Web site. You can also install MSI 4.5 directly from the vCenter Server `autorun.exe` installer.

vCenter Server Prerequisites

Before installing vCenter Server, review the prerequisites.

- Verify that you have the installation DVD, or download the vCenter Server installer from the VMware product page at http://www.vmware.com/products/.
- Verify that your hardware meets the vCenter Server hardware requirements.
- Verify that the fully qualified domain name (FQDN) of the system where you will install vCenter Server is resolvable. To check that the FQDN is resolvable, type **`nslookup`** ***`your_vCenter_Server_fqdn`*** at a command line prompt. If the FQDN is resolvable, the **`nslookup`** command returns the IP and name of the domain controller machine.

- Verify that DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server. When you install vCenter Server, the installation of the web server component that supports the vSphere Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server from its IP address. Reverse lookup is implemented using PTR records. To create a PTR record, see the documentation for your vCenter Server host operating system.
- Verify that the host name of the machine that you are installing vCenter Server on complies with RFC 952 guidelines.
- The installation path of vCenter Server must be compatible with the installation requirements for Microsoft Active Directory Application Mode (ADAM/AD LDS). The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).
- If the machine that you are installing vCenter Server on has VirtualCenter installed, you might want to upgrade instead of performing a fresh installation of vCenter Server.

  IMPORTANT To keep your existing VirtualCenter configuration, see the *vSphere Upgrade* documentation.

- Verify that no Network Address Translation (NAT) exists between the vCenter Server system and the hosts it will manage.
- For small-scale deployments, VMware recommends installing the bundled SQL Server 2008 R2 Express database on one of the supported operating systems.
- If the system that you use for your vCenter Server installation belongs to a workgroup rather than a domain, not all functionality is available to vCenter Server. If assigned to a workgroup, the vCenter Server system is not able to discover all domains and systems available on the network when using some features. To determine whether the system belongs to a workgroup or a domain, right-click **My Computer**. Click **Properties** and click the **Computer Name** tab. The **Computer Name** tab displays either a Workgroup label or a Domain label.
- During the installation, verify that the connection between the machine and the domain controller is working.
- Verify that the computer name is no more than 15 characters.
- The NETWORK SERVICE account is required on the folder in which vCenter Server is installed and on the HKLM registry.
- Verify that the DNS name of the machine matches the actual computer name.
- Make sure the system on which you are installing vCenter Server is not an Active Directory domain controller.
- On each system that is running vCenter Server, make sure that the domain user account has the following permissions:
  - **Member of the Administrators group**
  - **Act as part of the operating system**
  - **Log on as a service**
- Install vCenter Server, like any other network server, on a machine with a fixed IP address and well-known DNS name, so that clients can reliably access the service. Assign a static IP address and host name to the Windows server that will host the vCenter Server system. This IP address must have a valid (internal) domain name system (DNS) registration. Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Clients. Ensure that the vCenter Server has a valid

DNS resolution from all ESXi hosts and all vSphere Clients. If you use DHCP instead of a static IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Ping the computer name to test this connection. For example, if the computer name is `host-1.company.com`, run the following command in the Windows command prompt:

```
ping host-1.company.com
```

If you can ping the computer name, the name is updated in DNS.

Install vCenter Server

vCenter Server allows you to centrally manage hosts from either a physical or virtual Windows machine, and enables the use of advanced features such as vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), vSphere vMotion, vSphere Storage vMotion, and vSphere Auto Deploy.

Prerequisites

See "vCenter Server Prerequisites," on page 23.

vCenter Server requires the Microsoft .NET 3.5 SP1 Framework. If your system does not have it installed, the vCenter Server installer installs it. The .NET 3.5 SP1 installation might require Internet connectivity to download more files.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Server**™.

3 Follow the prompts in the installation wizard to choose the installer language, agree to the end user patent and license agreements, enter your user name, organization name, and license key.

If you omit the license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.

4 Click **Install SQL Server 2008 Express instance (for small-scale deployments)**.

This database is suitable for small deployments of up to 5 hosts and 50 virtual machines.

5 Select **Use SYSTEM Account** and click **Next**.

The Fully Qualified Domain Name field displays the FQDN of the system that you are installing vCenter Server on. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message is displayed when you click **Next**. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.

6 Accept the default destination folders and click **Next**.

7 Select **Create a standalone VMware vCenter Server instance** and click **Next**.

8 For each component that you install, accept the default port numbers and click **Next**.

If another service is using the defaults, specify alternative port and proxy information.

9 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the *vCenter Server Hardware Requirements* topic in *System Requirements*.

10 (Optional) In the Ready to Install the Program window, select **Select to bump up the ephemeral port value**.

This option increases the number of available ephemeral ports. If your vCenter Server manages hosts on which you will power on more than 2000 virtual machines simultaneously, this option prevents the pool of available ephemeral ports from being exhausted.

11 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

12 Click **Finish**.

What to do next

After you complete the installation, use the vSphere Client to connect to vCenter Server.

Start the vSphere Client and Log In to vCenter Server

When you connect to vCenter Server with the vSphere Client, you can manage vCenter Server as well as all of the hosts and virtual machines that it manages.

Procedure

1 Select **Start > Programs > VMware > VMware vSphere Client**.

2 Log in to vCenter Server as the administrator.

a Enter the IP address or vCenter Server name.

b Enter your Windows administrator user name.

c Enter your Windows administrator password.

3 Click **Login**.

You are connected to vCenter Server.

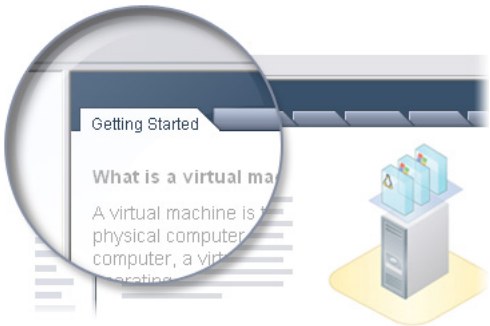
What to do next

Use the **Getting Started** tabs to create a datacenter.

Set Up a Basic Inventory with the Getting Started Tabs

When you connect to a vCenter Server instance with no objects in the inventory, the **Getting Started** tabs in the vSphere Client provide a wizard to help you set up a basic inventory quickly. There are no objects in the inventory when you connect to vCenter Server for the first time after installation.

Figure 3-2. vSphere Client Getting Started Tab



The **Getting Started** tabs wizard appears only if there are no objects in the inventory. After you have set up the basic inventory, the **Getting Started** tabs continue to provide information about the selected inventory object but no longer provide inventory setup wizard help.

Procedure

1 Create a Datacenter on page 27

The first step in setting up your vSphere environment is to create a datacenter.

2 Add a Host on page 28

When you add a host to a datacenter, vCenter Server manages it.

3 Create a Virtual Machine on page 28

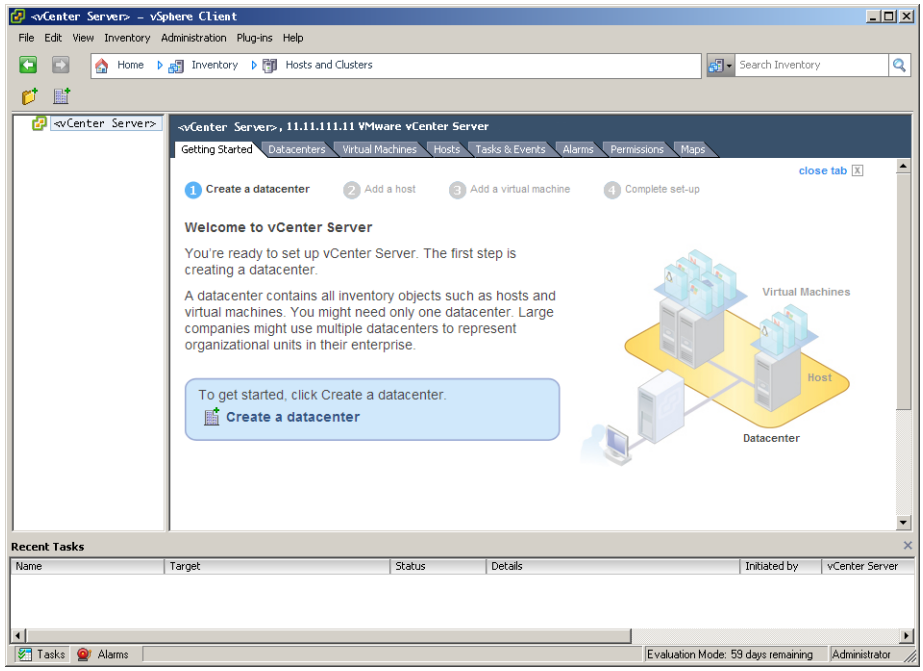
Creating a virtual machine is like building a computer, in which you determine things like disk size, and prepare it for receiving an operating system.

Create a Datacenter

The first step in setting up your vSphere environment is to create a datacenter.

If you are logging in for the first time, there are no inventory items in the Inventory panel.

Figure 3-3. vCenter Server with No Inventory Objects and the First Step in the Getting Started Tab Wizard



Procedure

1 On the **Getting Started** tab in the Information panel, follow the on-screen instructions and click **Create a datacenter**.

This creates a datacenter.

2 Name the datacenter by selecting it and entering a name.

What to do next

After you create a datacenter, add the ESXi host to it.

Add a Host

When you add a host to a datacenter, vCenter Server manages it.

Procedure

1 In the Inventory panel, select the datacenter you created if it is not selected.

2 On the **Getting Started** tab, follow the on-screen instructions and click **Add a host**.

   a Type the IP address or name of the ESXi host in the **Host** name field.

   b Enter the Username and Password for a user account that has administrative privileges on the selected managed host.

3 Click **Next**.

4 To confirm the Host Summary information, click **Next**.

5 Assign an existing license key to the host and click **Next**.

6 Click **Next**.

7 Select a location from the list of inventory objects and click **Next**.

8 Click **Finish** to complete adding a host.

   The vSphere Client displays a progress bar in the Recent Tasks pane while the host is added. Adding a new host can take a few minutes and the Status percentage might appear to pause at different increments during the process.

   When a new host is added, the host might appear as disconnected until vCenter Server completes the task. After the host is added, the status changes to connected, indicating that the host connection is complete.

The host that you installed and setup earlier and the virtual appliance that you imported are added to the inventory managed by vCenter Server.

What to do next

You already have a virtual machine in the inventory because you added the host with the virtual appliance to vCenter Server. Now create a new virtual machine.

Create a Virtual Machine

Creating a virtual machine is like building a computer, in which you determine things like disk size, and prepare it for receiving an operating system.

After you finish creating a virtual machine using this procedure, you must install a guest operating system, applications, and VMware Tools on it to perform work.

Prerequisites

A datacenter in the vCenter Server inventory.

An ISO image and a license for the operating system to install on the virtual machine.

Procedure

1 Click Hosts and Clusters on the vCenter Server Home page.

2 In the Inventory panel, select the host.

3 Click **Create a new virtual machine** on the **Getting Started** tab.

4 Select **Typical** and click **Next**.

5 Type a virtual machine name, select an inventory location, and click **Next**.

6 Select a datastore in which to store the virtual machine files and click **Next**.

The datastore must be large enough to hold the virtual machine and all of its virtual disk files.

7 Under **Guest Operating System**, select the operating system family (Microsoft Windows, Linux, or other) and select the version from the drop-down list.

This is the operating system for your virtual machine. Base your choice on your planned use of the virtual machine.

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

8 Keep the default Network configuration and click **next**.

9 Specify the size of the virtual disk, select **Thin Provision**, and click **Next**.

Enter the disk size in megabytes (MB) or gigabytes (GB). The virtual disk must be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.

10 On the Ready to Complete New Virtual Machine page, review your selections and click **Finish** to create the new virtual machine.

What to do next

After you create the virtual machine, you next install a guest operating system and VMware Tools on it. You can find instructions for how to install a guest operating system and VMware Tools in the vSphere Tutorial accessible from the vSphere Client. Select the virtual machine and follow the links on the **Getting Started** tab to learn how to install an operating system.

Where to Go Next

You have set up your vSphere environment. From here, you can expand your environment and your knowledge of vSphere capabilities.

- Expand your virtual infrastructure capacity by adding more hosts and storage.
- Expand your virtual datacenter by creating and importing new virtual machines.

For more information about how to evaluate the features and benefits of vSphere, go to http://www.vmware.com/tryvmware.

The vSphere Tutorial

The vSphere tutorial contains information about many of the basic vSphere components and tasks.

You can access the tutorial through the **Explore Further** links on the **Getting Started** tabs in the vSphere Client when you want learn more about the object that you selected in the inventory.

You can also access the tutorial from the **Help** menu in the vSphere Client.

vSphere Documentation

Refer to the VMware vSphere Documentation Center for information on advanced host and vCenter Server configuration, setup for larger deployments for production environments, as well as information on advanced vSphere features.

The vSphere Documentation Center consists of the combined vCenter Server and ESXi documentation set. To access the current versions of this and other publications, go to the vSphere Documentation Center on the VMware Web site.

Replacing Default vCenter Server Certificates

4

vSphere encrypts session information using standard digital certificates. Using the default certificates that vSphere creates might not comply with the security policy of your organization. If you require a certificate from a trusted certificate authority, you can replace the default certificate.

Certificate checking is enabled by default and SSL certificates are used to encrypt network traffic. However, ESXi uses automatically generated certificates that are created as part of the installation process and stored on the server system. These certificates are unique and make it possible to begin using the server, but they are not verifiable and are not signed by a trusted-well-known certificate authority (CA). These default certificates are vulnerable to possible man-in-the-middle attacks.

To receive the full benefit of certificate checking, especially if you intend to use encrypted remote connections externally, purchase a certificate from a trusted security authority or install new certificates that are signed by a valid internal certificate authority.

For more information about encryption and securing your vSphere environment, see the *vSphere Security* documentation.

This chapter includes the following topics:

vCenter Server Certificate Requirements

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components.

For example, communications between a vCenter Server system and each ESXi host that it manages are encrypted, and some features, such as vSphere Fault Tolerance, require the certificate verification provided by SSL. The client verifies the authenticity of the certificate presented during the SSL handshake phase, before encryption, which protects against "man-in-the-middle" attacks.

When you replace default vCenter Server certificates, the certificates you obtain for your servers must be signed and conform to the Privacy Enhanced Mail (PEM) key format. PEM is a key format that stores data in a Base-64 encoded Distinguished Encoding Rules (DER) format.

The key used to sign certificates must be a standard RSA key with an encryption length that ranges from 512 to 4096 bits. The recommended length is 2048 bits.

Certificates signed by a commercial certificate authority, such as Entrust or Verisign, are pre-trusted on the Windows operating system. However, if you replace a certificate with one signed by your own local root CA, or if you plan to continue using a default certificate, you must pre-trust the certificate by importing it into the local certificate store for each vSphere Client instance.

You must pre-trust all certificates that are signed by your own local root CA, unless you pre-trust the parent certificate, the root CA's own certificate. You must also pre-trust any valid default certificates that you will continue to use on vCenter Server.

Replace Default Server Certificates with Certificates Signed by a Commercial Certificate Authority

VMware recommends that you replace default certificates with those signed by a commercial certificate authority.

When you replace default server certificates in a production environment, deploy new certificates in stages, rather than all at the same time. Make sure that you understand the process as it applies to your environment before you replace certificates.

Prerequisites

Obtain certificates from a commercial certificate authority.

Procedure

1 Edit the OpenSSL Configuration File on page 32

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that are created during installation process. You can use OpenSSL to create certificate-signing requests (CSRs).

2 Create Certificate-Signing Requests for vCenter Server on page 33

You must generate a certificate-signing request (CSR) for each system that requires a replacement certificate.

3 Create the PFX File on page 33

The `rui.pfx` file is a concatenation of the system's certificate and private key, exported in the PFX format. The file is copied to the subdirectory on the vCenter Server system.

4 Load Replacement Certificates into Memory on page 34

The replacement certificate reencrypts all host passwords and the database password by using the new certificate.

Edit the OpenSSL Configuration File

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that are created during installation process. You can use OpenSSL to create certificate-signing requests (CSRs).

The examples used in this task and the other tasks in the certificate documentation are run from a Windows host machine and assume that the OpenSSL home directory is `c:\openssl\bin`.

The default OpenSSL installation includes a configuration file, `openssl.cnf`, located in the `\bin` directory. You can preconfigure settings in this configuration file, and you can overwrite default values by passing values to the command line. The syntax examples assume the following settings in the OpenSSL configuration file.

- The *$dir* variable is set to the local (.) directory path.
- The [req] section of the `openssl.cnf` has a *default_keyfile* variable set to *$dir/rui.key*.
- The [CA] section references a CA_default section.
- The [CA_default] section references a private_key named myroot.key.

Prerequisites

Download OpenSSL from http://www.openssl.org.

Procedure

1 Navigate to the OpenSSL directory.

2 Edit the OpenSSL configuration file (`openssl.cnf`), and enter the details appropriate for your environment.

Create Certificate-Signing Requests for vCenter Server

You must generate a certificate-signing request (CSR) for each system that requires a replacement certificate.

See the OpenSSL documentation at http://www.openssl.org for information about OpenSSL commands and options.

Prerequisites

Edit your OpenSSL configuration file (openssl.cnf) to suit your environment.

Procedure

1 Generate the RSA key for the vCenter Server system and the CSR.

For example:

```
openssl req –new –nodes –out mycsr.csr –config openssl.cnf
```

2 When prompted, type the fully qualified host name as the system's commonName.

3 Send the certificate request to the commercial certificate authority of your choice and wait for the return of the signed certificate.

Or, sign the request using your local root certificate authority:

```
openssl ca –out rui.crt –config openssl.cnf –infiles mycsr.csr
```

4 At the prompt, type the password needed to access the root key.

You have a new generated and signed `rui.crt` for the specified system, and the private key for the system (`rui.key`).

Create the PFX File

The `rui.pfx` file is a concatenation of the system's certificate and private key, exported in the PFX format. The file is copied to the subdirectory on the vCenter Server system.

Personal Information Exchange Format (PFX) enables transfer of certificates and their private keys from one computer to another or to removable media. The Microsoft Windows CryptoAPI uses the PFX format, also known as PKCS #12.

Procedure

- Export the certificate and key file together to PFX format using OpenSSL.

```
openssl pkcs12 –export –in rui.crt –inkey rui.key –name rui –passout pass:testpassword –out rui.pfx
```

IMPORTANT You must use the password **`testpassword`**.

Load Replacement Certificates into Memory

The replacement certificate reencrypts all host passwords and the database password by using the new certificate.

Use a browser to connect to the vCenter Server system and view the existing certificate. Take a screenshot or otherwise record the details of the existing certificate. After you load the new certificates into memory, you can use the screenshot to verify that the certificate was successfully replaced by comparing the old certificate to the new certificate. The method to view the certificate varies depending on the browser you are using. See your browser's documentation for more information.

Prerequisites

Verify that you have administrator privileges on the system.

Acquire or generate the following files:

- X.509 certificate file with RSA public key in PEM format, named `rui.crt`
- RSA private key in PEM format, named `rui.key`
- PKCS12 bundle of the same certificate and key, named `rui.pfx`

NOTE You do not need to update the keystore files `sms.keystore` and `sms.truststore`. SMS populates these files.

Procedure

1 Use a browser to connect to the vCenter Server system and view the existing certificate.

  The method to view the certificate varies depending on the browser you are using. See your browser's documentation for more information.

2 Take a screenshot or otherwise record the details of the existing certificate.

  After you load the new certificates into memory, you can use the screenshot to verify that the certificate was successfully replaced by comparing the old certificate to the new certificate.

3 On the server system, locate the SSL directory for vCenter Server.

  - For Windows 2008, the location is typically `C:\Program Data\VMware\VMware VirtualCenter\SSL`.
  - For Windows 2003, the location is typically `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`.

4 Back up the three existing certificate files: `rui.crt`, `rui.key`, and `rui.pfx`.

5 Copy the new certificate files into the SSL directory, overwriting the existing certificates.

6 Using a browser on the vCenter Server system, connect to
`http://localhost/mob/?moid=vpxd-securitymanager&vmodl=1`

  If you use a browser on another system, connect to
`https://`*`vSphere_server_system`*`/mob/?moid=vpxd-securitymanager&vmodl=1`

7 Enter the administrator name and password for the vCenter Server system.

  The Managed Object Type: vpxSecurityManager Web page appears.

8 Under Methods, click **reloadSslCertificate**.

9 Click **Invoke Method**.

  The following message appears: `Method Invocation Result: void.`

10 On the vCenter Server system, restart VMware vCenter Management Webservices.

   Linked Mode and other features will not function if you do not restart this service. Because the certificate thumbprint is published as Linked Mode shared information, it might take some time to replicate to the other vCenter Server instances in the Linked Mode group.

11 Replace the certificate used by the vCenter Server Inventory Service.

   a Copy `rui.key`, `rui.crt`, and `rui.pfx` to the vCenter Server Inventory Service installation directory.

   For example, `C:\Program Files\VMware\Infrastructure\Inventory Service\SSL\`.

   b Restart the Inventory Service using the Control Panel on the Windows system.

12 Refresh the page in the browser window and verify that the new certificate is installed by comparing it to the old certificate you recorded in Step 2.

If you installed the new certificate successfully, all host passwords and the database password are reencrypted using the new certificate. If your installation was unsuccessful (for example, the new certificate does not appear to load, vCenter Server cannot connect to managed hosts, or vCenter Server cannot connect to the database), see the *vSphere Troubleshooting* documentation.

Replace Default Server Certificates with Self-Signed Certificates

You can use OpenSSL to create keys and certificates and a root Certificate Authority (CA).

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that vSphere creates during the installation process. VMware recommends that you install certificates that are signed by a commercial Certificate Authority (CA). However, you have the option to use OpenSSL to create keys and certificates and a root CA, if appropriate. You can download OpenSSL from http://www.openssl.org.

The examples are run from a Windows host machine and assume that the OpenSSL home directory is `c:\openssl\bin`.

Inside the `openssl\bin` directory, you can create subdirectories to contain your keys, certificates, and other files. The syntax examples that appear assume a flat directory structure.

The instructions assume that a single, self-signed root CA is used to sign all certificate signing requests (CSRs).

Prerequisites

To create your own root CA and keys, secure the host system that you use to create local root CA certificate and its private key. The private key associated with the root CA must remain private.

VMware recommends creating keys, CSRs, and other security-related artifacts on trusted, air-gapped physical hardware over which you have complete control. VMware also recommends using a hardware RNG (random-number generator) to generate random numbers that have the appropriate characteristics (sufficient degree of entropy, for example) for cryptographic purposes.

Procedure

1 Edit the OpenSSL Configuration File on page 36

   VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that are created during installation process. You can use OpenSSL to create certificate-signing requests (CSRs).

2 Create a Local Root CA on page 36

   To replace the default certificates with certificates signed by your own local CA, you must create a root CA.

3 Create Certificate-Signing Requests for vCenter Server on page 37

You must generate a certificate-signing request (CSR) for each system that requires a replacement certificate.

4 Create Self-Signed Certificates on page 37

If you choose to install self-signed certificates, you can create them using OpenSSL.

5 Create the PFX File on page 38

The `rui.pfx` file is a concatenation of the system's certificate and private key, exported in the PFX format. The file is copied to the subdirectory on the vCenter Server system.

6 Load Replacement Certificates into Memory on page 38

The replacement certificate reencrypts all host passwords and the database password by using the new certificate.

Edit the OpenSSL Configuration File

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that are created during installation process. You can use OpenSSL to create certificate-signing requests (CSRs).

The examples used in this task and the other tasks in the certificate documentation are run from a Windows host machine and assume that the OpenSSL home directory is `c:\openssl\bin`.

The default OpenSSL installation includes a configuration file, `openssl.cnf`, located in the `\bin` directory. You can preconfigure settings in this configuration file, and you can overwrite default values by passing values to the command line. The syntax examples assume the following settings in the OpenSSL configuration file.

- The *$dir* variable is set to the local (.) directory path.
- The [req] section of the `openssl.cnf` has a *default_keyfile* variable set to *$dir/rui.key*.
- The [CA] section references a CA_default section.
- The [CA_default] section references a private_key named myroot.key.

Prerequisites

Download OpenSSL from http://www.openssl.org.

Procedure

1 Navigate to the OpenSSL directory.

2 Edit the OpenSSL configuration file (`openssl.cnf`), and enter the details appropriate for your environment.

Create a Local Root CA

To replace the default certificates with certificates signed by your own local CA, you must create a root CA.

The root CA's certificate must then be installed in any client systems that will connect to the managed hosts. Assuming you use the same root CA key to sign all the CSRs, you will have only one root CA certificate to install in the Windows clients.

Procedure

- Create a new root CA and an RSA key using OpenSSL. For example:

```
C:\OpenSSL\bin>openssl req –new –x509 –extensions v3_ca –keyout myroot.key –out myroot.crt –
days 3650 –config openssl.cnf
```

Create Certificate-Signing Requests for vCenter Server

You must generate a certificate-signing request (CSR) for each system that requires a replacement certificate.

See the OpenSSL documentation at http://www.openssl.org for information about OpenSSL commands and options.

Prerequisites

Edit your OpenSSL configuration file (openssl.cnf) to suit your environment.

Procedure

1 Generate the RSA key for the vCenter Server system and the CSR.

For example:

```
openssl req –new –nodes –out mycsr.csr –config openssl.cnf
```

2 When prompted, type the fully qualified host name as the system's commonName.

3 Send the certificate request to the commercial certificate authority of your choice and wait for the return of the signed certificate.

Or, sign the request using your local root certificate authority:

```
openssl ca –out rui.crt –config openssl.cnf –infiles mycsr.csr
```

4 At the prompt, type the password needed to access the root key.

You have a new generated and signed `rui.crt` for the specified system, and the private key for the system (`rui.key`).

Create Self-Signed Certificates

If you choose to install self-signed certificates, you can create them using OpenSSL.

Procedure

1 Create a text file named openssl.cnf with the configuration settings shown in the following example.

NOTE Modify all entries so they are specific to your environment. Providing the `commonName` is mandatory.

```
[req]
default_bits            = 2048
default_keyfile         = rui.key
distinguished_name      = req_distinguished_name
#Don't encrypt the key
encrypt_key             = no
prompt                  = no
string_mask             = nombstr

[ req_distinguished_name ]
countryName             = US
stateOrProvinceName     = California
localityName            = Palo Alto
0.organizationName      = VMware, Inc.
emailAddress            = ssl-certificates@vmware.com
commonName              = NAME_OF_SERVER_THAT_WILL_HAVE_CERTIFICATE
```

2 Create the self-signed certificate (`rui.key` and `rui.crt`) by running the following command.

```
openssl req -nodes -new -x509 -keyout rui.key -out rui.crt -days 3650 -config openssl.cnf
```

NOTE This command assumes that the `openssl.cnf` file is in the same folder as where the certificate is generated. If the certificate is in another folder, supply the full patch with the `openssl.cnf` file name.

3 Create backups of the original, default certificate and key to a safe location, in case you have problems and must restore your system to its previous state.

4 Copy the newly generated self-signed certificate (rui.key and rui.crt) to the default location for vCenter Server certificates.

- For Windows Server 2003, `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\`
- For Windows Server 2008, `C:\Program Data\VMware\VMware VirtualCenter\SSL\`

Create the PFX File

The `rui.pfx` file is a concatenation of the system's certificate and private key, exported in the PFX format. The file is copied to the subdirectory on the vCenter Server system.

Personal Information Exchange Format (PFX) enables transfer of certificates and their private keys from one computer to another or to removable media. The Microsoft Windows CryptoAPI uses the PFX format, also known as PKCS #12.

Procedure

◆ Export the certificate and key file together to PFX format using OpenSSL.

```
openssl pkcs12 -export -in rui.crt -inkey rui.key -name rui -passout pass:testpassword -out rui.pfx
```

IMPORTANT You must use the password **`testpassword`**.

Load Replacement Certificates into Memory

The replacement certificate reencrypts all host passwords and the database password by using the new certificate.

Use a browser to connect to the vCenter Server system and view the existing certificate. Take a screenshot or otherwise record the details of the existing certificate. After you load the new certificates into memory, you can use the screenshot to verify that the certificate was successfully replaced by comparing the old certificate to the new certificate. The method to view the certificate varies depending on the browser you are using. See your browser's documentation for more information.

Prerequisites

Verify that you have administrator privileges on the system.

Acquire or generate the following files:

- X.509 certificate file with RSA public key in PEM format, named `rui.crt`
- RSA private key in PEM format, named `rui.key`
- PKCS12 bundle of the same certificate and key, named `rui.pfx`

NOTE You do not need to update the keystore files `sms.keystore` and `sms.truststore`. SMS populates these files.

Procedure

1 Use a browser to connect to the vCenter Server system and view the existing certificate.

The method to view the certificate varies depending on the browser you are using. See your browser's documentation for more information.

2 Take a screenshot or otherwise record the details of the existing certificate.

After you load the new certificates into memory, you can use the screenshot to verify that the certificate was successfully replaced by comparing the old certificate to the new certificate.

3 On the server system, locate the SSL directory for vCenter Server.

- For Windows 2008, the location is typically `C:\Program Data\VMware\VMware VirtualCenter\SSL`.
- For Windows 2003, the location is typically `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`.

4 Back up the three existing certificate files: `rui.crt`, `rui.key`, and `rui.pfx`.

5 Copy the new certificate files into the SSL directory, overwriting the existing certificates.

6 Using a browser on the vCenter Server system, connect to
`http://localhost/mob/?moid=vpxd-securitymanager&vmodl=1`

If you use a browser on another system, connect to
`https://`*`vSphere_server_system`*`/mob/?moid=vpxd-securitymanager&vmodl=1`

7 Enter the administrator name and password for the vCenter Server system.

The Managed Object Type: vpxSecurityManager Web page appears.

8 Under Methods, click **reloadSslCertificate**.

9 Click **Invoke Method**.

The following message appears: `Method Invocation Result: void.`

10 On the vCenter Server system, restart VMware vCenter Management Webservices.

Linked Mode and other features will not function if you do not restart this service. Because the certificate thumbprint is published as Linked Mode shared information, it might take some time to replicate to the other vCenter Server instances in the Linked Mode group.

11 Replace the certificate used by the vCenter Server Inventory Service.

a Copy `rui.key`, `rui.crt`, and `rui.pfx` to the vCenter Server Inventory Service installation directory.

For example, `C:\Program Files\VMware\Infrastructure\Inventory Service\SSL\`.

b Restart the Inventory Service using the Control Panel on the Windows system.

12 Refresh the page in the browser window and verify that the new certificate is installed by comparing it to the old certificate you recorded in Step 2.

If you installed the new certificate successfully, all host passwords and the database password are reencrypted using the new certificate. If your installation was unsuccessful (for example, the new certificate does not appear to load, vCenter Server cannot connect to managed hosts, or vCenter Server cannot connect to the database), see the *vSphere Troubleshooting* documentation.

Using Host Profiles to Ensure Identical Directory Service Settings for Multiple Hosts

5

The vSphere host profiles feature reduces the manual steps that are involved in configuring a host and can help maintain consistency and correctness across the datacenter. This can be particularly helpful when ensuring identical security settings across multiple hosts.

Host profiles simplify host configuration management through user-defined configuration policies. The host profile policies capture the blueprint of a known, validated host configuration, and use this configuration to configure networking, storage, security, and other settings across multiple hosts. For example, you can create a host profile to enable you to specify how a host joins a directory service domain.

When you use a directory service such as Active Directory to authenticate users, you can create a host profile that enables you to apply directory service settings to many hosts at the same time. For example, you can specify that the hosts to which the profile applies use vSphere Authentication Proxy to add the host to a domain.

NOTE Hosts must be in maintenance mode before you apply a host profile.

Specify How a Host Joins a Directory Service

You can use host profiles to specify how hosts join a directory service domain. Hosts can join with user-supplied Active Directory credentials or can join using the vSphere Authentication Proxy server (CAM server).

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

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

Procedure

1 Create a Host Profile from Host Profiles View on page 42

   You can create a host profile from the Host Profiles main view using the configuration of an existing host.

2 Place a Host in Maintenance Mode on page 42

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

3 Select the Join Domain Method on page 43

   Specify how hosts will join a directory service domain: with user-supplied Active Directory credentials or by using the vSphere Authentication Proxy server (CAM server).

4 Attach Profiles from the Host on page 43

   Before you can apply the profile to a host you need to attach the host to the profile or the profile to the host.

5 Apply a Profile from the Host Profiles View on page 44

You can apply a profile to a host from the Host Profiles main view.

Create a Host Profile from Host Profiles View

You can create a host profile from the Host Profiles main view using the configuration of an existing host.

Prerequisites

You must have a vSphere installation and at least one properly configured host in the inventory.

Procedure

1 In the Host Profiles main view, click **Create Profile**.

The Create Profile wizard appears.

2 Select the option to create a new profile and click **Next**.

3 Select the host you want to designate as the reference host for the new host profile and click **Next**.

The reference host must be a valid host.

4 Type the name and enter a description for the new profile and click **Next**.

5 Review the summary information for the new profile and click **Finish** to complete creating the profile.

The new profile appears in the profile list.

Place a Host in Maintenance Mode

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

Virtual machines that are running on a host entering maintenance mode need to be migrated to another host (either manually or automatically by DRS) or shut down. The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered down or migrated to different hosts. You cannot power on virtual machines or migrate virtual machines to a host entering maintenance mode.

When no more running virtual machines are on the host, the host's icon changes to include **under maintenance** and the host's Summary panel indicates the new state. While in maintenance mode, the host does not allow you to deploy or power on a virtual machine.

NOTE DRS does not recommend (or perform, in fully automated mode) any virtual machine migrations off of a host entering maintenance or standby mode if the vSphere HA failover level would be violated after the host enters the requested mode.

Procedure

1 In the vSphere Client inventory, right-click a host and select **Enter Maintenance Mode**.

- If the host is part of a partially automated or manual DRS cluster, a list of migration recommendations for virtual machines running on the host appears.
- If the host is part of an automated DRS cluster, virtual machines are migrated to different hosts when the host enters maintenance mode.

2 If applicable, click **Apply Recommendations**.

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

Select the Join Domain Method

Specify how hosts will join a directory service domain: with user-supplied Active Directory credentials or by using the vSphere Authentication Proxy server (CAM server).

Prerequisites

- If the host is using a CA-signed certificate and is not provisioned by Auto Deploy, verify that the certificate has been added to the local trust certificate store on the vSphere Authentication Proxy server system. See the *vSphere Security* documentation.
- If DHCP is configured for the management interface, verify that the DHCP range is set. See the *vSphere Security* documentation.

Procedure

1. Using the vSphere Client, select **View > Management > Host Profiles**.
2. Right-click an existing host profile and select **Edit Profile**.
3. Expand the profile tree, and then expand **Authentication configuration**.
4. Expand **Active Directory configuration** and select **Domain Name**.
5. Select **Configure a fixed domain name** and enter the domain where the host will join.
6. Click **OK**.
7. Expand **Active Directory configuration** and select **JoinDomain Method**.
8. On the **Configuration Details** tab in the right pane, select the method used to join the host to the domain.
   - To use the vSphere Authentication Proxy (CAM server), select **Use CAM service to join the host to domain** and enter the IP address of the authentication proxy server.
   - To use Active Directory credentials, select **Use user specified AD credentials to join the host to domain**.
9. Click **OK**.

Attach Profiles from the Host

Before you can apply the profile to a host you need to attach the host to the profile or the profile to the host.

You can attach a profile to a host from the host's context menu in the Hosts and Clusters inventory view.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remain.

Procedure

1. In the Host and Clusters view, select the host to which you want to attach a profile.
2. Right-click the host and select **Host Profile > Manage Profile**.

   NOTE If no host profiles exist in your inventory, a dialog appears asking if you want to create and attach the host to this profile.

3. In the Attach Profile dialog, select the profile to attach to the host and click **OK**.

The host profile is updated in the **Summary** tab of the host.

Apply a Profile from the Host Profiles View

You can apply a profile to a host from the Host Profiles main view.

Prerequisites

The profile must be attached to the host and the host must be in maintenance mode before a profile is applied to it.

Procedure

1 In the Host Profiles main view, select the profile you want to apply to the host.

2 Select the **Hosts and Clusters** tab.

The list of attached hosts are shown under Entity Name.

3 Click **Apply Profile**.

In the Profile Editor, you might be prompted to enter the required parameters needed to apply the profile.

4 Enter the parameters and click **Next**.

5 Continue until all the required parameters are entered.

6 Click **Finish**.

Compliance Status is updated.

Configuring iSCSI Adapters for Hosts to Access vSphere Shared Storage 6

With shared networked storage in vSphere you can aggregate storage resources to be more flexible when provisioning the resources to virtual machines. One approach to shared storage is an iSCSI storage area network (SAN), to which you connect using either hardware or software adapters.

Without access to shared storage, the virtual machines on a host are limited to the host's physical hard disk to contain the virtual machines' virtual disks. If you have centralized and aggregated storage resources, it releases virtual machines from depending on local storage. Multiple hosts can access datastores on networked storage concurrently.

ESXi supports iSCSI technology that enables a host to use an IP network to access remote storage. iSCSI technology includes software iSCSI adapters and hardware iSCSI adapters.

Software iSCSI adapter VMware code that is built into the VMkernel. Your host can connect to the iSCSI storage device through standard network adapters. The software iSCSI adapter handles iSCSI processing while communicating with the network adapter. With the software iSCSI adapter, you can use iSCSI technology without specialized hardware.

Hardware iSCSI adapter Third-party adapter that offloads iSCSI and network processing from your host. A dependent hardware iSCSI adapter depends on vSphere networking and management interfaces provided by VMware. An independent hardware iSCSI adapter implements its own networking and iSCSI configuration and management interfaces.

For information about the storage options available in vSphere, see the *vSphere Storage* documentation.

To get access to remote iSCSI devices, you must configure iSCSI adapters according to their type. Follow one of two configuration workflows to configure either software iSCSI adapters or hardware iSCSI adapters.

This chapter includes the following topics:

Configure Software iSCSI Adapters

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

Before you can use the software iSCSI adapter, you configure it by activating the adapter and setting up its networking.

Prerequisites

Designate a separate network adapter for iSCSI. Do not use iSCSI on 100Mbps or slower adapters.

Procedure

1 Activate the Software iSCSI Adapter on page 46

You must activate your software iSCSI adapter so that your host can use it to access iSCSI storage.

2 Create Network Connections for iSCSI on page 46

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

Activate the Software iSCSI Adapter

You must activate your software iSCSI adapter so that your host can use it to access iSCSI storage.

You can activate only one software iSCSI adapter.

Prerequisites

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

NOTE If you boot from iSCSI using the software iSCSI adapter, the adapter is enabled and the network configuration is created at the first boot. If you disable the adapter, it is reenabled each time you boot the host.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

3 Click **Add** and select **Software iSCSI Adapter**.

The software iSCSI adapters appears on the list of storage adapters.

4 Select the iSCSI adapter from the list and click **Properties**.

5 Click **Configure**.

6 Make sure that the adapter is enabled and click **OK**.

After enabling the adapter, the host assigns the default iSCSI name to it. If you change the default name, follow iSCSI naming conventions.

After you activate the adapter, you can disable it, but you cannot remove it from the list of storage adapters.

Create Network Connections for iSCSI

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

The following tasks discuss the iSCSI network configuration with a vSphere standard switch.

If you use a vSphere distributed switch with multiple uplink ports, for port binding, create a separate distributed port group per each physical NIC. Then set the team policy so that each distributed port group has only one active uplink port. For detailed information on vSphere distributed switches, see the *vSphere Networking* documentation.

Procedure

1 Create a Single VMkernel Adapter for iSCSI on page 47

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

2 (Optional) Create Additional VMkernel Adapters for iSCSI on page 48

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

3 Change Port Group Policy for iSCSI VMkernel Adapters on page 49

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

4 Bind iSCSI Adapters with VMkernel Adapters on page 49

Bind an iSCSI adapter with a VMkernel adapter.

Create a Single VMkernel Adapter for iSCSI

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 In the vSphere Standard Switch view, click **Add Networking**.

4 Select **VMkernel** and click **Next**.

5 Select **Create a vSphere standard switch** to create a new standard switch.

6 Select a NIC to use for iSCSI traffic.

IMPORTANT If you are creating a VMkernel interface for the dependent hardware iSCSI adapter, select the NIC that corresponds to the iSCSI component. See "Determine Association Between iSCSI and Network Adapters," on page 51.

7 Click **Next**.

8 Enter a network label.

A network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, iSCSI.

9 Click **Next**.

10 Specify the IP settings and click **Next**.

11 Review the information and click **Finish**.

You created the virtual VMkernel adapter for a physical network adapter on your host.

What to do next

If your host has one physical network adapter for iSCSI traffic, you must bind the virtual adapter that you created to the iSCSI adapter.

If you have multiple network adapters, create additional VMkernel adapters and then perform iSCSI binding. The number of virtual adapters must correspond to the number of physical adapters on the host.

(Optional) Create Additional VMkernel Adapters for iSCSI

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

Prerequisites

You must create a vSphere standard switch that maps an iSCSI VMkernel adapter to a single physical NIC designated for iSCSI traffic.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 Connect additional network adapters to the standard switch.

   a In the standard switch Properties dialog box, click the **Network Adapters** tab and click **Add**.

   b Select one or more NICs from the list and click **Next**.

   With dependent hardware iSCSI adapters, select only those NICs that have a corresponding iSCSI component.

   c Review the information on the Adapter Summary page and click **Finish**.

   The list of network adapters reappears, showing the network adapters that the vSphere standard switch now claims.

5 Create iSCSI VMkernel adapters for all NICs that you added.

   The number of VMkernel interfaces must correspond to the number of NICs on the vSphere standard switch.

   a In the standard switch Properties dialog box, click the **Ports** tab and click **Add**.

   b Select **VMkernel** and click **Next**.

   c Under **Port Group Properties**, enter a network label, for example iSCSI, and click **Next**.

   d Specify the IP settings and click **Next**.

   When you enter the subnet mask, make sure that the NIC is set to the subnet of the storage system it connects to.

   e Review the information and click **Finish**.

CAUTION If the NIC you use with your iSCSI adapter, either software or dependent hardware, is not in the same subnet as your iSCSI target, your host cannot establish sessions from this network adapter to the target.

What to do next

Change the network policy for all VMkernel adapters, so that it is compatible with the network binding requirements. You can then bind the iSCSI VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Change Port Group Policy for iSCSI VMkernel Adapters

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

By default, for each virtual adapter on the vSphere standard switch, all network adapters appear as active. You must override this setup, so that each VMkernel interface maps to only one corresponding active NIC. For example, vmk1 maps to vmnic1, vmk2 maps to vmnic2, and so on.

Prerequisites

Create a vSphere standard switch that connects VMkernel with physical network adapters designated for iSCSI traffic. The number of VMkernel adapters must correspond to the number of physical adapters on the vSphere standard switch.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 On the **Ports** tab, select an iSCSI VMkernel adapter and click **Edit**.

5 Click the **NIC Teaming** tab and select **Override switch failover order**.

6 Designate only one physical adapter as active and move all remaining adapters to the **Unused Adapters** category.

7 Repeat Step 4 through Step 6 for each iSCSI VMkernel interface on the vSphere standard switch.

What to do next

After you perform this task, bind the virtual VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Bind iSCSI Adapters with VMkernel Adapters

Bind an iSCSI adapter with a VMkernel adapter.

Prerequisites

Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

The list of available storage adapters appears.

3 Select the software or dependent iSCSI adapter to configure and click **Properties**.

4 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

5 Click **Add** and select a VMkernel adapter to bind with the iSCSI adapter.

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

6 Click **OK**.

The network connection appears on the list of VMkernel port bindings for the iSCSI adapter.

7 Verify that the network policy for the connection is compliant with the binding requirements.

Configure Dependent Hardware iSCSI Adapters

A dependent hardware iSCSI adapter is a third-party adapter that relies on VMware networking and iSCSI configuration.

An example of a dependent iSCSI adapter is a Broadcom 5709 NIC. When installed on a host, it presents its two components, a standard network adapter and an iSCSI engine, to the same port. The iSCSI engine appears on the list of storage adapters as an iSCSI adapter. Although the dependent iSCSI adapter is enabled by default, you must take action to make it functional. First, through a virtual VMkernel interface, you connect it to a physical network adapter associated with it. You can then configure the dependent iSCSI adapter.

Procedure

1 View Dependent Hardware iSCSI Adapters on page 50

View a dependent hardware iSCSI adapter to verify that it is correctly loaded.

2 Determine Association Between iSCSI and Network Adapters on page 51

You create network connections to bind dependent iSCSI and network adapters. To create the connections correctly, you must determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.

3 Create Network Connections for iSCSI on page 51

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

View Dependent Hardware iSCSI Adapters

View a dependent hardware iSCSI adapter to verify that it is correctly loaded.

If the dependent hardware adapter does not appear on the list of storage adapters, check whether it needs to be licensed. See your vendor documentation.

Prerequisites

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Storage Adapters** in the Hardware panel.

If it is installed, the dependent hardware iSCSI adapter appears on the list of storage adapters under such category as, for example, Broadcom iSCSI Adapter.

3 Select the adapter to view and click **Properties**.

The iSCSI Initiator Properties dialog box opens. It displays the default details for the adapter, including the iSCSI name, iSCSI alias, and the status.

4 (Optional) To change the default iSCSI name, click **Configure**.

What to do next

Although the dependent iSCSI adapter is enabled by default, to make it functional, you must set up networking for the iSCSI traffic and bind the adapter to the appropriate VMkernel iSCSI port. You then configure discovery addresses and CHAP parameters.

Determine Association Between iSCSI and Network Adapters

You create network connections to bind dependent iSCSI and network adapters. To create the connections correctly, you must determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.

Prerequisites

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

Procedure

1 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

2 Click **Add**.

The network adapter, for example vmnic2, that corresponds to the dependent iSCSI adapter is listed.

What to do next

You must bind the associated dependent hardware iSCSI and network adapters by creating the network connections.

Create Network Connections for iSCSI

Configure connections for the traffic between the software or dependent hardware iSCSI adapters and the physical network adapters.

The following tasks discuss the iSCSI network configuration with a vSphere standard switch.

If you use a vSphere distributed switch with multiple uplink ports, for port binding, create a separate distributed port group per each physical NIC. Then set the team policy so that each distributed port group has only one active uplink port. For detailed information on vSphere distributed switches, see the *vSphere Networking* documentation.

Procedure

1 Create a Single VMkernel Adapter for iSCSI on page 51

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

2 (Optional) Create Additional VMkernel Adapters for iSCSI on page 52

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

3 Change Port Group Policy for iSCSI VMkernel Adapters on page 53

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

4 Bind iSCSI Adapters with VMkernel Adapters on page 54

Bind an iSCSI adapter with a VMkernel adapter.

Create a Single VMkernel Adapter for iSCSI

You must connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 In the vSphere Standard Switch view, click **Add Networking**.

4 Select **VMkernel** and click **Next**.

5 Select **Create a vSphere standard switch** to create a new standard switch.

6 Select a NIC to use for iSCSI traffic.

IMPORTANT If you are creating a VMkernel interface for the dependent hardware iSCSI adapter, select the NIC that corresponds to the iSCSI component. See "Determine Association Between iSCSI and Network Adapters," on page 51.

---

7 Click **Next**.

8 Enter a network label.

A network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, iSCSI.

9 Click **Next**.

10 Specify the IP settings and click **Next**.

11 Review the information and click **Finish**.

You created the virtual VMkernel adapter for a physical network adapter on your host.

What to do next

If your host has one physical network adapter for iSCSI traffic, you must bind the virtual adapter that you created to the iSCSI adapter.

If you have multiple network adapters, create additional VMkernel adapters and then perform iSCSI binding. The number of virtual adapters must correspond to the number of physical adapters on the host.

(Optional) Create Additional VMkernel Adapters for iSCSI

Use this task if you have two or more physical network adapters for iSCSI and you want to connect all of your NICs to a single vSphere standard switch. In this task, you add NICs and VMkernel adapters to an existing vSphere standard switch.

Prerequisites

You must create a vSphere standard switch that maps an iSCSI VMkernel adapter to a single physical NIC designated for iSCSI traffic.

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 Connect additional network adapters to the standard switch.

a In the standard switch Properties dialog box, click the **Network Adapters** tab and click **Add**.

b Select one or more NICs from the list and click **Next**.

With dependent hardware iSCSI adapters, select only those NICs that have a corresponding iSCSI component.

c Review the information on the Adapter Summary page and click **Finish**.

The list of network adapters reappears, showing the network adapters that the vSphere standard switch now claims.

5 Create iSCSI VMkernel adapters for all NICs that you added.

The number of VMkernel interfaces must correspond to the number of NICs on the vSphere standard switch.

a In the standard switch Properties dialog box, click the **Ports** tab and click **Add**.

b Select **VMkernel** and click **Next**.

c Under **Port Group Properties**, enter a network label, for example iSCSI, and click **Next**.

d Specify the IP settings and click **Next**.

When you enter the subnet mask, make sure that the NIC is set to the subnet of the storage system it connects to.

e Review the information and click **Finish**.

CAUTION If the NIC you use with your iSCSI adapter, either software or dependent hardware, is not in the same subnet as your iSCSI target, your host cannot establish sessions from this network adapter to the target.

What to do next

Change the network policy for all VMkernel adapters, so that it is compatible with the network binding requirements. You can then bind the iSCSI VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Change Port Group Policy for iSCSI VMkernel Adapters

If you use a single vSphere standard switch to connect VMkernel to multiple network adapters, change the port group policy, so that it is compatible with the iSCSI network requirements.

By default, for each virtual adapter on the vSphere standard switch, all network adapters appear as active. You must override this setup, so that each VMkernel interface maps to only one corresponding active NIC. For example, vmk1 maps to vmnic1, vmk2 maps to vmnic2, and so on.

Prerequisites

Create a vSphere standard switch that connects VMkernel with physical network adapters designated for iSCSI traffic. The number of VMkernel adapters must correspond to the number of physical adapters on the vSphere standard switch.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab and click **Networking**.

3 Select the vSphere standard switch that you use for iSCSI and click **Properties**.

4 On the **Ports** tab, select an iSCSI VMkernel adapter and click **Edit**.

5 Click the **NIC Teaming** tab and select **Override switch failover order**.

6 Designate only one physical adapter as active and move all remaining adapters to the **Unused Adapters** category.

7 Repeat Step 4 through Step 6 for each iSCSI VMkernel interface on the vSphere standard switch.

What to do next

After you perform this task, bind the virtual VMkernel adapters to the software iSCSI or dependent hardware iSCSI adapters.

Bind iSCSI Adapters with VMkernel Adapters

Bind an iSCSI adapter with a VMkernel adapter.

Prerequisites

Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.

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

Procedure

1 Log in to the vSphere Client, and select a host from the inventory panel.

2 Click the **Configuration** tab, and click **Storage Adapters** in the Hardware panel.

The list of available storage adapters appears.

3 Select the software or dependent iSCSI adapter to configure and click **Properties**.

4 In the iSCSI Initiator Properties dialog box, click the **Network Configuration** tab.

5 Click **Add** and select a VMkernel adapter to bind with the iSCSI adapter.

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

6 Click **OK**.

The network connection appears on the list of VMkernel port bindings for the iSCSI adapter.

7 Verify that the network policy for the connection is compliant with the binding requirements.

Configuring Hosts or Clusters to Use vMotion for Increased Service Availability

7

With vSphere vMotion, you can migrate powered on virtual machines from one physical server to another without service interruption. The result is a more efficient assignment of resources, and you can avoid using an out-of-hours downtime model of maintenance.

When you use vMotion, you do not have to wait until a downtime window to perform maintenance. vMotion enables you to move a virtual machine from one host to another without powering off the virtual machine. You can use vMotion to move virtual machines off a host so that you can perform host maintenance without virtual machine downtime. You can perform fundamental maintenance during business hours without service interruption.

In addition, vSphere Distributed Resource Scheduler (DRS) uses vMotion to balance the resource load in clusters of physical hosts, managing a cluster as a single compute resource.

Before you can migrate a virtual machine with vMotion, you must configure both the source host and destination host. You can also configure a cluster of hosts for vMotion.

Whether you configure vMotion in hosts independently or within a cluster, vMotion has a set of requirements covering licenses, storage, and networking. See "Host Configuration Requirements for vMotion," on page 56.

Hosts and vMotion

Setting up a host for vMotion includes verifying that vMotion is licensed on the hosts, and configuring networking for either vSphere standard switches or vSphere distributed switches. See "Set Up a Host for vMotion," on page 58.

Clusters and vMotion

DRS places virtual machines so that the load across a cluster is balanced, and cluster-wide resource allocation policies (for example, reservations, priorities, and limits) are enforced. As cluster conditions change (for example, load and available resources), DRS uses vMotion to migrate virtual machines to other hosts as necessary.

Setting up a cluster for vMotion includes setting up individual hosts, but also entails creating the cluster and adding managed hosts to the cluster. See "Set Up a Cluster for vMotion," on page 62.

You use the Enhanced vMotion Compatibility (EVC) feature to ensure vMotion compatibility between the hosts in the cluster. See "About Enhanced vMotion Compatibility," on page 57.

This chapter includes the following topics:

Host Configuration Requirements for vMotion

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.

See "Set Up a Host for vMotion," on page 58 or "Set Up a Cluster for vMotion," on page 62.

Privilege Requirements for Managing Licenses for vMotion

To assign a license key so that vMotion appears as a licensed feature for a host, you must have the **Global.Licenses** privilege.

Administrator is the only vSphere default role with the **Global.Licenses** privilege. If you want someone other than an administrator to be able to assign license keys, you must add that privilege to an existing role or create a role for it.

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 *vSphere Storage* 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 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 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 standard switches 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 vSphere Distributed Switches for networking, ensure that source and destination hosts are members of all vSphere Distributed Switches that virtual machines use for networking.
- Use of Jumbo Frames is recommended for best vMotion performance.

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.
- 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 Requirements for vMotion," on page 56.
- All hosts in the cluster must have supported CPUs for the EVC mode you want to enable. To check EVC support for a specific processor or server 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.

Set Up a Host for vMotion

To migrate a virtual machine with vMotion, you must configure both the source and destination hosts.

After you make sure the hosts are licensed for vMotion, you configure networking on them to enable vMotion.

Procedure

1 Assign a License Key to an ESXi Host on page 58

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

2 Verify that vMotion Appears as a Licensed Feature on page 58

You must verify that vMotion is licensed on all the hosts whose resources you want to be available for dynamic reallocation.

3 Configure Networking for vMotion on page 59

You must choose whether to use vSphere standard switches or vSphere distributed switches for networking.

Assign a License Key to an ESXi Host

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

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

Prerequisites

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

Procedure

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

2 In the **Management** tab, right-click a host and select **Change license key**.

3 Assign a license key.

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

4 Click **OK**.

Verify that vMotion Appears as a Licensed Feature

You must verify that vMotion is licensed on all the hosts whose resources you want to be available for dynamic reallocation.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab.

3 Click **Licensed Features** under Software.

4 In the Product Features list, verify that vMotion is listed.

5 Repeat steps 1 through 4 until you have verified all applicable hosts.

Configure Networking for vMotion

You must choose whether to use vSphere standard switches or vSphere distributed switches for networking.

- With vSphere standard switches, each server has its own virtual switch: a vSphere standard switch handles network traffic at the host level in a vSphere environment. A vSphere standard switch can route traffic internally between virtual machines and link to external networks.
- A vSphere distributed switch treats the network as an aggregated resource, reducing the administrative burden resulting from per-host virtual switch configuration management. The single VDS spans multiple hosts at the datacenter level.
- A vSphere distributed switch maintains port statistics regardless of virtual machine location or vMotion migration history. With standard switches, such statistics are kept on a per-virtual-port basis and are lost during events like a vMotion migration.
- Set Up VMkernel Networking on a vSphere Standard Switch on page 59

  Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.
- Set Up VMkernel Networking on a vSphere Distributed Switch on page 61

  Create a VMkernel network adapter to use as a vMotion interface for hosts using vSphere Distributed Switches for networking.

Set Up VMkernel Networking on a vSphere Standard Switch

Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.

Procedure

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

2 Select the host in the inventory pane.

3 On the host **Configuration** tab, click **Networking**.

4 In the vSphere Standard Switch view, click **Add Networking**.

5 Select **VMkernel** and click **Next**.

6 Select the vSphere standard switch to use, or select **Create a vSphere standard switch** to create a new vSphere standard switch.

7 Select the check boxes for the network adapters for your vSphere standard switch to use.

  Select adapters for each vSphere standard switch so that virtual machines or other services that connect through the adapter can reach the correct Ethernet segment. If no adapters appear under Create a new vSphere standard switch, all the network adapters in the system are being used by existing vSphere standard switches or vSphere distributed switches. You can either create a vSphere standard switch without a network adapter, or select a network adapter that an existing vSphere standard switch uses.

8 Click **Next**.

9 Select or enter a network label and a VLAN ID.

Option	Description
Network Label	A name that identifies the port group that you are creating. This is the label that you specify when you configure VMkernel services such as vMotion and IP storage and you configure a virtual adapter to be attached to this port group.
VLAN ID	Identifies the VLAN that the port group's network traffic will use.

10 (Optional) Select **Use this port group for vMotion** to enable this port group to advertise itself to another host as the network connection through which vMotion traffic should be sent.

11 (Optional) Select **Use this port group for fault tolerance logging**.

12 (Optional) Select **Use this port group for management traffic**.

13 If IPv6 is enabled on the host, select **IP (Default)**, **IPv6**, or **IP and IPv6 networking**.

This option does not appear on hosts that do not have IPv6 enabled. IPv6 configuration cannot be used with dependent hardware iSCSI adapters.

14 Click **Next**.

15 Select how to obtain IP settings.

Option	Description
Obtain IP settings automatically	Use DHCP to obtain IP settings.
Use the following IP settings	Specify IP settings manually. a Enter the IP address and subnet mask for the VMkernel interface. b Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI. On the **DNS Configuration** tab, the name of the host is entered by default. The DNS server addresses that were specified during installation are also preselected, as is the domain. c Click **OK** and click **Next**.

16 If you are using IPv6 for the VMkernel interface, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.
Obtain IPv6 addresses automatically through router advertisement	Use router advertisement to obtain IPv6 addresses.
Static IPv6 addresses	a Click **Add** to add a new IPv6 address. b Enter the IPv6 address and subnet prefix length, and click **OK**. c To change the VMkernel default gateway, click **Edit**.

17 Click **Next**.

18 Review the information, click **Back** to change any entries, and click **Finish**.

Set Up VMkernel Networking on a vSphere Distributed Switch

Create a VMkernel network adapter to use as a vMotion interface for hosts using vSphere Distributed Switches for networking.

Procedure

1 Edit VMkernel Configuration on a vSphere Distributed Switch on page 61

You can edit a VMkernel virtual network adapter on a vSphere distributed switch to change the IP settings, such as IP address, subnet mask, default gateway, and DNS configuration. You can also select whether the virtual adapter is used for vMotion or fault tolerance logging.

2 Add Hosts to a vSphere Distributed Switch on page 62

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

Edit VMkernel Configuration on a vSphere Distributed Switch

You can edit a VMkernel virtual network adapter on a vSphere distributed switch to change the IP settings, such as IP address, subnet mask, default gateway, and DNS configuration. You can also select whether the virtual adapter is used for vMotion or fault tolerance logging.

Procedure

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

2 Select the host in the inventory pane.

3 On the host **Configuration** tab, click **Networking**.

4 Select the vSphere Distributed Switch view.

5 Click **Manage Virtual Adapters**.

6 Select the VMkernel adapter to modify and click **Edit**.

7 Under Network Connection, select **vSphere Distributed Switch** and **Port Group** or **Port** to add this virtual adapter to.

8 Select **Use this virtual adapter for vMotion** to enable this port group to advertise itself to another host as the network connection that vMotion traffic should be sent through.

You can enable this property for only one vMotion and IP storage port group for each host. If this property is not enabled for any port group, migration with vMotion to this host is not possible.

9 (Optional) Select **Use this virtual adapter for fault tolerance logging**.

10 (Optional) Select **Use this virtual adapter for management traffic**.

11 Under IP Settings, specify the **IP Address** and **Subnet Mask**, or select **Obtain IP settings automatically** .

12 Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI.

On the **DNS Configuration** tab, the name of the host appears in the name field by default. The DNS server addresses that were specified during installation are also preselected, as is the domain.

On the **Routing** tab, a gateway is needed for connectivity to machines not on the same IP subnet as the VMkernel.

Static IP settings is the default.

13 Use the up and down arrows to set the MTU for the VMkernel adapter.

14 Click **OK**.

Add Hosts to a vSphere Distributed Switch

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

Procedure

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

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

3 Select the hosts to add.

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

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

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

---

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

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

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

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

c Click **OK**.

7 Click **Next**.

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

a Select **Migrate virtual machine networking**.

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

9 Click **Next**.

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

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

Set Up a Cluster for vMotion

To take advantage of the increased service availability offered by vMotion, you can set up a cluster and enable vMotion for all the hosts in the cluster.

Prerequisites

Hosts must conform to the requirements described in "Host Configuration Requirements for vMotion," on page 56 and "EVC Requirements," on page 57.

Procedure

1 Create the Cluster to be Configured for EVC on page 63

VMware recommends creating an empty EVC cluster and moving hosts into it later as the simplest way of creating an EVC cluster with minimal disruption to your existing infrastructure.

2 Set Up a Host for vMotion on page 64

To migrate a virtual machine with vMotion, you must configure both the source and destination hosts.

3 Add a Managed Host to a Cluster on page 68

When you add a standalone host already being managed by vCenter Server to a DRS cluster, the host's resources become associated with the cluster.

Create the Cluster to be Configured for EVC

VMware recommends creating an empty EVC cluster and moving hosts into it later as the simplest way of creating an EVC cluster with minimal disruption to your existing infrastructure.

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 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**.

5 Enable EVC in the cluster by selecting the supported CPU for the hosts you will be adding.

Option	Description
Enable EVC for AMD Hosts	The EVC feature is enabled for AMD hosts.
Enable EVC for Intel® Hosts	The EVC feature is enabled for Intel hosts.

6 From the **VMware EVC Mode** drop-down menu, select the baseline CPU feature set to enable for the cluster.

If the selected EVC Mode cannot be selected, the Compatibility pane displays the reasons why and the relevant hosts for each reason.

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

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

The EVC cluster is added to the inventory.

What to do next

Set up hosts and add them to the cluster.

Set Up a Host for vMotion

To migrate a virtual machine with vMotion, you must configure both the source and destination hosts.

After you make sure the hosts are licensed for vMotion, you configure networking on them to enable vMotion.

Procedure

1 Assign a License Key to an ESXi Host on page 64

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

2 Verify that vMotion Appears as a Licensed Feature on page 64

You must verify that vMotion is licensed on all the hosts whose resources you want to be available for dynamic reallocation.

3 Configure Networking for vMotion on page 65

You must choose whether to use vSphere standard switches or vSphere distributed switches for networking.

Assign a License Key to an ESXi Host

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

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

Prerequisites

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

Procedure

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

2 In the **Management** tab, right-click a host and select **Change license key**.

3 Assign a license key.

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

4 Click **OK**.

Verify that vMotion Appears as a Licensed Feature

You must verify that vMotion is licensed on all the hosts whose resources you want to be available for dynamic reallocation.

Procedure

1 Log in to the vSphere Client and select the host from the inventory panel.

2 Click the **Configuration** tab.

3 Click **Licensed Features** under Software.

4 In the Product Features list, verify that vMotion is listed.

5 Repeat steps 1 through 4 until you have verified all applicable hosts.

Configure Networking for vMotion

You must choose whether to use vSphere standard switches or vSphere distributed switches for networking.

- With vSphere standard switches, each server has its own virtual switch: a vSphere standard switch handles network traffic at the host level in a vSphere environment. A vSphere standard switch can route traffic internally between virtual machines and link to external networks.
- A vSphere distributed switch treats the network as an aggregated resource, reducing the administrative burden resulting from per-host virtual switch configuration management. The single VDS spans multiple hosts at the datacenter level.
- A vSphere distributed switch maintains port statistics regardless of virtual machine location or vMotion migration history. With standard switches, such statistics are kept on a per-virtual-port basis and are lost during events like a vMotion migration.
- Set Up VMkernel Networking on a vSphere Standard Switch on page 65

  Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.
- Set Up VMkernel Networking on a vSphere Distributed Switch on page 66

  Create a VMkernel network adapter to use as a vMotion interface for hosts using vSphere Distributed Switches for networking.

Set Up VMkernel Networking on a vSphere Standard Switch

Create a VMkernel network adapter for use as a vMotion interface or an IP storage port group.

Procedure

1. Log in to the vSphere Client and select the **Hosts and Clusters** inventory view.
2. Select the host in the inventory pane.
3. On the host **Configuration** tab, click **Networking**.
4. In the vSphere Standard Switch view, click **Add Networking**.
5. Select **VMkernel** and click **Next**.
6. Select the vSphere standard switch to use, or select **Create a vSphere standard switch** to create a new vSphere standard switch.
7. Select the check boxes for the network adapters for your vSphere standard switch to use.

   Select adapters for each vSphere standard switch so that virtual machines or other services that connect through the adapter can reach the correct Ethernet segment. If no adapters appear under Create a new vSphere standard switch, all the network adapters in the system are being used by existing vSphere standard switches or vSphere distributed switches. You can either create a vSphere standard switch without a network adapter, or select a network adapter that an existing vSphere standard switch uses.
8. Click **Next**.
9. Select or enter a network label and a VLAN ID.

Option	Description
Network Label	A name that identifies the port group that you are creating. This is the label that you specify when you configure VMkernel services such as vMotion and IP storage and you configure a virtual adapter to be attached to this port group.
VLAN ID	Identifies the VLAN that the port group's network traffic will use.

10 (Optional) Select **Use this port group for vMotion** to enable this port group to advertise itself to another host as the network connection through which vMotion traffic should be sent.

11 (Optional) Select **Use this port group for fault tolerance logging**.

12 (Optional) Select **Use this port group for management traffic**.

13 If IPv6 is enabled on the host, select **IP (Default)**, **IPv6**, or **IP and IPv6 networking**.

This option does not appear on hosts that do not have IPv6 enabled. IPv6 configuration cannot be used with dependent hardware iSCSI adapters.

14 Click **Next**.

15 Select how to obtain IP settings.

Option	Description
Obtain IP settings automatically	Use DHCP to obtain IP settings.
Use the following IP settings	Specify IP settings manually. a Enter the IP address and subnet mask for the VMkernel interface. b Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI. On the **DNS Configuration** tab, the name of the host is entered by default. The DNS server addresses that were specified during installation are also preselected, as is the domain. c Click **OK** and click **Next**.

16 If you are using IPv6 for the VMkernel interface, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.
Obtain IPv6 addresses automatically through router advertisement	Use router advertisement to obtain IPv6 addresses.
Static IPv6 addresses	a Click **Add** to add a new IPv6 address. b Enter the IPv6 address and subnet prefix length, and click **OK**. c To change the VMkernel default gateway, click **Edit**.

17 Click **Next**.

18 Review the information, click **Back** to change any entries, and click **Finish**.

Set Up VMkernel Networking on a vSphere Distributed Switch

Create a VMkernel network adapter to use as a vMotion interface for hosts using vSphere Distributed Switches for networking.

Procedure

1 Edit VMkernel Configuration on a vSphere Distributed Switch on page 67

You can edit a VMkernel virtual network adapter on a vSphere distributed switch to change the IP settings, such as IP address, subnet mask, default gateway, and DNS configuration. You can also select whether the virtual adapter is used for vMotion or fault tolerance logging.

2 Add Hosts to a vSphere Distributed Switch on page 67

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

Edit VMkernel Configuration on a vSphere Distributed Switch

You can edit a VMkernel virtual network adapter on a vSphere distributed switch to change the IP settings, such as IP address, subnet mask, default gateway, and DNS configuration. You can also select whether the virtual adapter is used for vMotion or fault tolerance logging.

Procedure

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

2 Select the host in the inventory pane.

3 On the host **Configuration** tab, click **Networking**.

4 Select the vSphere Distributed Switch view.

5 Click **Manage Virtual Adapters**.

6 Select the VMkernel adapter to modify and click **Edit**.

7 Under Network Connection, select **vSphere Distributed Switch** and **Port Group** or **Port** to add this virtual adapter to.

8 Select **Use this virtual adapter for vMotion** to enable this port group to advertise itself to another host as the network connection that vMotion traffic should be sent through.

   You can enable this property for only one vMotion and IP storage port group for each host. If this property is not enabled for any port group, migration with vMotion to this host is not possible.

9 (Optional) Select **Use this virtual adapter for fault tolerance logging**.

10 (Optional) Select **Use this virtual adapter for management traffic**.

11 Under IP Settings, specify the **IP Address** and **Subnet Mask**, or select **Obtain IP settings automatically** .

12 Click **Edit** to set the VMkernel Default Gateway for VMkernel services, such as vMotion, NAS, and iSCSI.

   On the **DNS Configuration** tab, the name of the host appears in the name field by default. The DNS server addresses that were specified during installation are also preselected, as is the domain.

   On the **Routing** tab, a gateway is needed for connectivity to machines not on the same IP subnet as the VMkernel.

   Static IP settings is the default.

13 Use the up and down arrows to set the MTU for the VMkernel adapter.

14 Click **OK**.

Add Hosts to a vSphere Distributed Switch

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

Procedure

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

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

3 Select the hosts to add.

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

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

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

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

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

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

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

   c Click **OK**.

7 Click **Next**.

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

   a Select **Migrate virtual machine networking**.

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

9 Click **Next**.

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

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

Add a Managed Host to a Cluster

When you add a standalone host already being managed by vCenter Server to a DRS cluster, the host's resources become associated with the cluster.

You can decide whether you want to associate existing virtual machines and resource pools with the cluster's root resource pool or graft the resource pool hierarchy.

NOTE If a host has no child resource pools or virtual machines, the host's resources are added to the cluster but no resource pool hierarchy with a top-level resource pool is created.

Procedure

1 Select the host from either the inventory or list view.

2 Drag the host to the target cluster object.

3 Select what to do with the host's virtual machines and resource pools.

- **Put this host's virtual machines in the cluster's root resource pool**

  vCenter Server removes all existing resource pools of the host and the virtual machines in the host's hierarchy are all attached to the root. Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares after selecting this option, which destroys the resource pool hierarchy.

- **Create a resource pool for this host's virtual machines and resource pools**

  vCenter Server creates a top-level resource pool that becomes a direct child of the cluster and adds all children of the host to that new resource pool. You can supply a name for that new top-level resource pool. The default is **Grafted from <host_name>**.

The host is added to the cluster.

IT Request Fulfillment with a Library of Virtual Machine Templates

8

Having a library of virtual machine templates can be a major benefit for the IT provider and for the user. With a library of templates, most virtual machine requests can be fulfilled quickly with something ready to be deployed.

In providing virtual machines to fulfill user needs, it is not efficient to create each virtual machine as a custom job. The solution is to create a master image, a template, of a type of virtual machine, and deploy copies of the virtual machine as needed. You can anticipate the requests from your user population, and prepare families of templates to cover requests.

Constructing a Template Library

For example, you can have a family of templates running applications on Windows Servers 2008, another family for a Linux distribution, another family for Windows 7, and so on.

As an illustration, you might create a virtual machine with Windows Server 2008, with all patches and VMware Tools installed. You can clone the virtual machine and install application A on one clone and application B on the other. Convert them to templates to become part of your library. Keep the original virtual machine to use to make additional application-specific templates.

Table 8-1. Example Library of Templates

Windows Family Virtual Machine Templates	Linux Family Virtual Machine Templates
Windows 2008 Server R2 with SQL	Linux-based Apache Web server
Windows 2003 Server SP2 with SQL	Linux-based Tomcat server
Windows 2003 Server SP2 with DB2	Linux-based NFS server
Windows 2003 Server SP2 with Oracle 10g	Linux-based Samba server
Windows 2003 Server SP2 with Oracle 11g	Linux-based server for development environment
Windows 2008 Server R2 for development environment	Linux-based server for testing environment
Windows 2003 Server SP2 for development environment	Linux-based DHCP server
Windows 2008 Server R2 for testing environment	Linux-based domain server
Windows 2003 Server SP2 for testing environment	

Sample Process for Creating Templates and Deploying Virtual Machines

The first step is to create a virtual machine from scratch to be the starting point for developing the template. After installing a guest operating system in the virtual machine, you install an application. From there you can convert the virtual machine to a template, and from the template deploy virtual machines.

This scenario uses a rudimentary workflow, and includes the cloning step as optional. When you become familiar with the process, you can adapt it, using shortcuts where applicable to your situation, and you can expand it to include cloning if you skipped it the first time around.

Privileges Required for Creating Templates and Deploying Virtual Machines

The process of creating templates and deploying virtual machines can be done by someone who has been assigned the Administrator role. If you want to create a unique role for this process that does not include all the privileges of an Administrator, the following list contains the minimum necessary.

- **Virtual machine.Provisioning.Deploy template** on the template to deploy from the template.
- **Virtual machine.Provisioning.Create template from virtual machine** on the datacenter to create the template.
- **Virtual machine.Provisioning.Clone template** on the datacenter to clone a template to create other templates.
- **Virtual machine.Provisioning.Mark as virtual machine** on the datacenter to convert template to a virtual machine.
- **Virtual machine.Provisioning.Mark as template** on the virtual machine to convert it to a template.
- **Virtual machine.Inventory.Create new** on the destination folder or datacenter.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.

For information and instruction about privileges and roles, see the *vSphere Security* documentation.

Create Templates and Deploy Virtual Machines From Them

Follow the workflow in the sample tasks in this scenario to become familiar with the process for deploying virtual machines from templates.

Procedure

1 Create a Virtual Machine to Use as the Template on page 71

To deploy virtual machines from a template, you must first create the basic virtual machine from which the templates are converted.

2 Installing a Guest Operating System on page 75

A virtual machine is not complete until you install the guest operating system and VMware Tools. Installing a guest operating system in your virtual machine is essentially the same as installing it in a physical computer.

3 Create Virtual Machine Clones on Which to Install Other Applications on page 76

When you have created a virtual machine with a guest operating system, you can clone that virtual machine to create a family of templates with that guest operating system. but each template having a different application installed.

4 Install Applications for Your Future Templates on page 77

Before you convert the virtual machine to a template, you must install the application that fulfills the role of the virtual machines that are to be deployed from the template.

5 Convert a Virtual Machine to a Template in the vSphere Client on page 77

You can convert a virtual machine directly to a template instead of making a copy by cloning.

6 Deploy a Virtual Machine from a Template in the vSphere Client on page 77

Deploying a virtual machine from a template creates a new virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties configured for the template.

7 Customize the Guest Operating System After Deploying the Virtual Machine on page 80

When you deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties. These properties include the computer name, network settings, and license settings.

Create a Virtual Machine to Use as the Template

To deploy virtual machines from a template, you must first create the basic virtual machine from which the templates are converted.

For this example procedure, disregard the optional steps in "Select a Datastore in the vSphere Client," on page 73. You do not need to add memory or CPUs in "Select an Operating System in the vSphere Client," on page 74, and you can disregard the optional steps in "Complete Virtual Machine Creation in the vSphere Client," on page 74.

Procedure

1 Start the Virtual Machine Creation Process in the vSphere Client on page 72

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

2 Select the Typical Configuration Path for the New Virtual Machine on page 72

For this example procedure, use the typical configuration to simplify the workflow.

3 Enter a Name and Location for the Virtual Machine in the vSphere Client on page 73

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

4 Select a Host or Cluster in the vSphere Client on page 73

You can place the virtual machine in a cluster or on a host that is not in a cluster.

5 Select a Datastore in the vSphere Client on page 73

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

6 Select an Operating System in the vSphere Client on page 74

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

7 Complete Virtual Machine Creation in the vSphere Client on page 74

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

What to do next

Install a guest operating system.

Start the Virtual Machine Creation Process in the vSphere Client

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

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

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

Prerequisites

Verify that you have the following privileges:

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

Procedure

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

   The New Virtual Machine wizard opens.

What to do next

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

Select the Typical Configuration Path for the New Virtual Machine

For this example procedure, use the typical configuration to simplify the workflow.

The first step in the New Virtual Machine wizard is to select the configuration path to follow. The choice is either **Typical** or **Custom**. The typical path contains fewer pages and options.

For information about the custom configuration path, see the *vSphere Virtual Machine Administration* documentation.

Procedure

- Select **Typical** on the Configuration page of the New Virtual Machine wizard and click **Next**.

The Name and Location page opens.

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

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

The name can be up to 80 characters long. If you are connected to vCenter Server and have folders in your inventory, names must be unique within the folder. Names are not case-sensitive, so the name `my_vm` is identical to `My_Vm`.

Prerequisites

Verify that you have an appropriate naming strategy in place.

Procedure

1 On the Name and Location page of the New Virtual Machine wizard, type a name.

2 Select a folder or the root of the datacenter.

3 Click **Next**.

The Host / Cluster or the Resource Pool page opens.

Select a Host or Cluster in the vSphere Client

You can place the virtual machine in a cluster or on a host that is not in a cluster.

A cluster is a collection of ESXi hosts and associated virtual machines with shared resources and a shared management interface. Grouping hosts into clusters allows you to enable many optional features that enhance the availability and flexibility of your infrastructure.

Procedure

1 On the Host / Cluster page of the New Virtual Machine wizard, select the host or cluster where you want to run the virtual machine.

2 Click **Next**.

If resource pools are configured on the host, the Resource Pool page opens. Otherwise, the Datastore page opens.

What to do next

Select a resource pool or a datastore on which to run the virtual machine.

Select a Datastore in the vSphere Client

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

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

Procedure

1 On the Storage page of the New Virtual Machine wizard, select a datastore in which to store the virtual machine files.

2 (Optional) To turn off Storage DRS for the virtual machine, select **Disable Storage DRS for this virtual machine**.

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

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

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

4 Click **Next**.

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

Select an Operating System in the vSphere Client

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

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

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

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

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

Procedure

1 On the Guest Operating System page of the New Virtual Machine wizard, select an operating system family.

2 Select an operating system and version from the drop-down menu and click **Next**.

If you selected a Novell NetWare guest operating system, the Memory page opens. If any of the total cores available on the host, the maximum virtual CPUs supported by the virtual machine hardware version, or the maximum supported CPUs on the guest operating system equal 1, the virtual machine CPU count is set to 1 and the Memory page opens.

3 If you selected **Other (32-bit)** or **Other (64-bit)**, enter a name for the operating system in the text box.

4 Click **Next**.

What to do next

You can add memory or CPUs for the virtual machine.

Complete Virtual Machine Creation in the vSphere Client

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

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

Procedure

1 On the Ready to Complete page of the New Virtual Machine wizard, review the configuration settings for the virtual machine.

2 (Optional) Select **Edit the virtual machine settings before completion** and click **Continue**.

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

3 (Optional) Click **Cancel** to go back and review the wizard settings.

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

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

What to do next

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

Installing a Guest Operating System

A virtual machine is not complete until you install the guest operating system and VMware Tools. Installing a guest operating system in your virtual machine is essentially the same as installing it in a physical computer.

The basic steps for a typical operating system are described in this section. See *VMware Guest Operating System Installation* on the VMware website for more information about individual guest operating systems.

Install a Guest Operating System from Media

You can install a guest operating system from a CD-ROM or from an ISO image. Installing from an ISO image is typically faster and more convenient than a CD-ROM installation.

If the virtual machine's boot sequence progresses too quickly for you to open a console to the virtual machine and enter BIOS or EFI setup, you might need to delay the boot order. See the *vSphere Virtual Machine Administration* documentation.

Prerequisites

- Verify that the installation ISO image is present on a VMFS datastore or network file system (NFS) volume accessible to the ESXi host.
- Verify that you have the installation instructions that the operating system vendor provides.

Procedure

1 Open the vSphere Client and log in to the vCenter Server system or host on which the virtual machine resides.

2 Select an installation method.

Option	Action
CD-ROM	Insert the installation CD-ROM for your guest operating system into the CD-ROM drive of your ESXi host.
ISO image	a Right-click the virtual machine in the inventory list and select **Edit Settings**. b Click the **Hardware** tab and select **CD/DVD Drive**. c In the Device Type panel, select **Datastore ISO File** and browse for the ISO image for your guest operating system.

3 Right-click the virtual machine and select **Power > Power On**.

A green right arrow appears next to the virtual machine icon in the inventory list.

4 Follow the installation instructions that the operating system vendor provides.

What to do next

Install VMware Tools. Installing VMware Tools in the guest operating system is important. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience without them. See the *Installing and Configuring VMware Tools* documentation.

Create Virtual Machine Clones on Which to Install Other Applications

When you have created a virtual machine with a guest operating system, you can clone that virtual machine to create a family of templates with that guest operating system. but each template having a different application installed.

You clone the virtual machine to have fresh copies of the virtual machine with the guest operating system that you installed. Later, you install different applications in each of the clones to fill out your template library.

NOTE If you are proceeding through the workflow as an exercise with the goal of one virtual machine at the end, you can skip this step.

Procedure

1 Right-click the template and select **Clone**.

2 Give the new template a unique name and description and click **Next**.

3 Select the host or cluster and click **Next**.

4 Select a datastore for the template and click **Next**.

5 Specify in which format to store the template's virtual disks.

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

6 Click **Next**.

7 Review the information for the template and click **Finish**.

You cannot use the new template until the cloning task completes.

vCenter Server adds the cloned template to the list in the **Virtual Machines** tab.

What to do next

Repeat for as many templates you need for the library with the operating system you installed earlier.

Install an application so that you can convert a complete virtual machine to a template.

Install Applications for Your Future Templates

Before you convert the virtual machine to a template, you must install the application that fulfills the role of the virtual machines that are to be deployed from the template.

Prerequisites

You have created a virtual machine and have installed a guest operating system in it.

Procedure

- Follow the application's installation instructions that come with the media for the application.

What to do next

Convert the virtual machine to a template.

Convert a Virtual Machine to a Template in the vSphere Client

You can convert a virtual machine directly to a template instead of making a copy by cloning.

When you convert a virtual machine to a template, you cannot edit or power on the template unless you convert it back to a virtual machine.

Prerequisites

- You must be connected to vCenter Server to convert a virtual machine to a template. You cannot create templates if you connect the vSphere Client directly to an ESXi host.
- Before you convert a virtual machine to a template, select it in the inventory and power it off.

Procedure

- Right-click the virtual machine and select **Template > Convert to Template**.

  vCenter Server marks that virtual machine as a template and displays the task in the Recent Tasks pane.

Deploy a Virtual Machine from a Template in the vSphere Client

Deploying a virtual machine from a template creates a new virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties configured for the template.

Table 8-2. Selections to Make For the Purposes of This Example

Step in the procedure	Option to select
3	**Run the virtual machine on a standalone host**
5	**Store all virtual machines in the same location on a datastore**
6	**Same format as source**
7	**Customize using the Customization Wizard**
8	**Power on this virtual machine after creation**

Prerequisites

- Verify that you are connected to vCenter Server. You cannot work with templates if you connect the vSphere Client directly to an ESXi host.
- You must be connected to vCenter Server to deploy a virtual machine from a template. You cannot deploy from a template if you connect the vSphere Client directly to an ESXi host.

- To customize the guest operating system of the virtual machine, check that your guest operating system meets the requirements for customization. See "Guest Operating System Customization Requirements," on page 80.
- To use a customization specification, you must first create or import the customization specification.

Procedure

1 Right-click the template, and select **Deploy Virtual Machine from this Template**.

2 Enter a virtual machine name, select a location, and click **Next**.

3 Select a host or cluster on which to run the new virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click **Next**. b Select a host within the cluster and click **Next**.

4 Select a resource pool in which to run the virtual machine and click **Next**.

5 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a (Optional) Apply a virtual machine storage profile for the virtual machine home files and the virtual disks from the **VM Storage Profile** drop-down menu. The list of datastores shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a (Optional) Apply a virtual machine storage profile for the virtual machine home files and the virtual disks from the **VM Storage Profile** drop-down menu. The list of datastores shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. b Select a datastore cluster. c (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. d Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c (Optional) Apply a virtual machine storage profile from the **VM Storage Profile** drop-down menu. The list of datastores shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. d (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. e Click **Next**.

6 Select the format for the virtual machine's disks and click **Next**.

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

7 Select a guest operating system customization option.

Option	Description
Do not customize	Select **Do not customize** and click **Next**. Does not customize any of the guest operating system settings. All settings remain identical to those of the source virtual machine.
Customize using the Customization Wizard	Opens the Customization Wizard so that you can select customization options for the guest operating system. Select this option and click **Next** to launch the Customization Wizard. ■ To customize a Linux guest operating system, see "Customize Linux During Cloning or Deployment in the vSphere Client," on page 84. ■ To customize a Windows guest operating system, see "Customize Windows During Cloning or Deployment in the vSphere Client," on page 81.
Customize using an existing customization specification	Uses the settings in a saved customization specification to customize the guest operating system. a Select **Customize using an existing customization specification**. b Select the customization specification that you want to use. c (Optional) Select **Use the Customization Wizard to temporarily adjust the specification before deployment** if you want to make changes to the specification for this deployment only. d Click **Next**.

8 Review your selections and select whether to power on the virtual machine or edit virtual machine settings.

Option	Action
Power on this virtual machine after creation	Select this option and click **Finish**. The virtual machine powers on after the deployment task completes.
Edit virtual hardware	a Select this option and click **Continue**. b In the Virtual Machine Properties dialog box, make any changes and click **OK**.

Option	Action
Show all storage recommendations	This option appears only when the virtual machine disks are stored on a datastore cluster and Storage DRS is enabled. When you select this option, the Virtual Machine Storage Placement Recommendations dialog box appears when you click **Continue**. The dialog box lists the datastores in the datastore cluster that are recommended for virtual machine placement.
Edit Storage DRS rules	This option appears only when the virtual machine disks are stored on a datastore cluster. This option is selected when you select **Edit virtual hardware**. You can edit Storage DRS rules on the **Options** tab of the Virtual Machine Properties dialog box. When you select the **Edit Storage DRS rules** check box, the Storage DRS rules dialog box appears when you click **Continue**.

The virtual machine is deployed. You cannot use or edit the virtual machine until the deployment is complete. This might take several minutes if the deployment involves creating a virtual disk.

Customize the Guest Operating System After Deploying the Virtual Machine

When you deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties. These properties include the computer name, network settings, and license settings.

Customizing guest operating systems can help prevent conflicts that can result if virtual machines with identical settings are deployed, such as conflicts due to duplicate computer names.

The customization requirements and procedures for Windows and for Linux are different.

- Guest Operating System Customization Requirements on page 80

  To customize the guest operating system, you must configure the virtual machine and guest to meet VMware Tools and virtual disk requirements. Other requirements apply, depending on the guest operating system type.

- Customize Windows During Cloning or Deployment in the vSphere Client on page 81

  When you deploy a new virtual machine from a template or clone an existing virtual machine, you can customize Windows guest operating systems for the virtual machine.

- Customize Linux During Cloning or Deployment in the vSphere Client on page 84

  In the process of deploying a new virtual machine from a template or cloning an existing virtual machine, you can customize Linux guest operating systems for the virtual machine.

Guest Operating System Customization Requirements

To customize the guest operating system, you must configure the virtual machine and guest to meet VMware Tools and virtual disk requirements. Other requirements apply, depending on the guest operating system type.

VMware Tools Requirements

The current version of VMware Tools must be installed on the virtual machine or template to customize the guest operating system during cloning or deployment.

Virtual Disk Requirements

The guest operating system being customized must be installed on a disk attached as SCSI node 0:0 in the virtual machine configuration.

Windows Requirements

Customization of Windows guest operating systems requires the following conditions:

- Microsoft Sysprep tools must be installed on the vCenter Server system. See the *vSphere Virtual Machine Administration* documentation.
- The ESXi host that the virtual machine is running on must be 3.5 or later.

Guest operating system customization is supported on multiple Windows operating systems.

Linux Requirements

Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system.

Guest operating system customization is supported on multiple Linux distributions.

Verifying Customization Support for a Guest Operating System

To verify customization support for Windows operating systems or Linux distributions and compatible ESXi hosts, see the *VMware Compatibility Guide* at VMware.com. You can use this online tool to search for the guest operating system and ESXi version. After the tool generates your list, click the guest operating system to see whether guest customization is supported.

Customize Windows During Cloning or Deployment in the vSphere Client

When you deploy a new virtual machine from a template or clone an existing virtual machine, you can customize Windows guest operating systems for the virtual machine.

NOTE The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine boots the first time after customization.

Prerequisites

Verify that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 80.

Start the Guest Customization wizard when you deploy from a template. See "Deploy a Virtual Machine from a Template in the vSphere Client," on page 77.

Procedure

1. On the Guest Customization page of the Clone Virtual Machine wizard, select **Customize using the Customization Wizard** and click **Next**.
2. Type the virtual machine owner's name and organization and click **Next**.

3 Enter the guest operating system's computer name and click **Next**.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are case-insensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.
Enter a name in the Deploy wizard	The vSphere Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

4 Provide licensing information for the Windows operating system and click **Next**.

Option	Action
For non-server operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	a Type the Windows product key for the new guest operating system. b Select **Include Server License Information**. c Select either **Per seat** or **Per server**. d (Optional) If you selected **Per server**, enter the maximum number of simultaneous connections for the server to accept.

5 Configure the administrator password for the virtual machine and click **Next**.

a Type a password for the administrator account and confirm the password by typing it again.

NOTE You can change the administrator password only if the administrator password on the source Windows virtual machine is blank. If the source Windows virtual machine or template already has a password, the administrator password does not change.

b (Optional) To log users into the guest operating system as Administrator, select the check box, and select the number of times to log in automatically.

6 Select the time zone for the virtual machine and click **Next**.

7 (Optional) On the **Run Once** page, specify commands to run the first time a user logs into the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for more information on Run Once commands.

8 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) to open the Network Properties dialog box. c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

9 Select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, MSHOME.
Windows Server Domain	a Type the domain name. b Type the user name and password for a user account that has permission to add a computer to the specified domain.

10 (Optional) Select Generate New Security ID (SID) and click **Next**.

A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

11 Save the customized options as an `.xml` file.

a Select **Save this customization specification for later use**.

b Specify the filename for the specification and click **Next**.

12 Click **Finish** to save your changes.

You return to the Deploy Template or Clone Virtual Machine wizard. The customization is carried out after you complete the Deploy Template or Clone Virtual Machine wizard.

When the new virtual machine boots for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might reboot a number of times during this process.

If the guest operating system pauses when the new virtual machine boots, it might be waiting for you to correct errors, such as an incorrect product key or invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

After you deploy and customize versions of Windows XP or Windows 2003 that are not volume licensed, you might need to reactivate your operating system on the new virtual machine.

If the new virtual machine encounters customization errors while it is booting, the errors are logged to `%WINDIR%\temp\vmware-imc`. To view the error log file, click the Windows **Start** button and select **Programs > Administrative Tools > Event Viewer**.

Customize Linux During Cloning or Deployment in the vSphere Client

In the process of deploying a new virtual machine from a template or cloning an existing virtual machine, you can customize Linux guest operating systems for the virtual machine.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 80.

To perform this procedure, launch the Customization wizard when deploying from a template. See "Deploy a Virtual Machine from a Template in the vSphere Client," on page 77.

Procedure

1 On the Guest Customization page of the Clone Virtual Machine wizard, select **Customize using the Customization Wizard** and click **Next**.

2 Specify how to determine the host name to identify the guest operating system on the network.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are case-insensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 15 characters, it is truncated.
Enter a name in the Deploy wizard	The vSphere Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

3 Enter the **Domain Name** for the computer and click **Next**.

4 Select the time zone for the virtual machine and click **Next**.

5 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) to open the Network Properties dialog box. c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

6 Enter DNS and domain settings.

7 Save the customized options as an `.xml` file.

   a Select **Save this customization specification for later use**.

   b Specify the filename for the specification and click **Next**.

8 Click **Finish** to save your changes.

You return to the Deploy Template or Clone Virtual Machine wizard. The customization is carried out after you complete the Deploy Template or Clone Virtual Machine wizard.

When the new virtual machine boots for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might reboot a number of times during this process.

If the guest operating system pauses when the new virtual machine boots, it might be waiting for you to correct errors, such as an incorrect product key or invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

If the new virtual machine encounters customization errors while it is booting, the errors are reported using the guest's system logging mechanism. View the errors by opening `/var/log/vmware-imc/toolsDeployPkg.log`.

Creating a Role that Permits Completion of a Limited Task

9

You can configure vSphere so that identified users can perform only a specific and focused function. This protects your system from errors that might be made by users who are in unfamiliar or sensitive parts of the system's interface.

If you follow the tenets of role-based access control (RBAC), you would create roles for particular job functions, and give each role a subset of permissions or privileges needed to do a function and no more. This protects the system from errors, while simplifying an administrator's task in assigning permissions.

vSphere provides the ability to achieve role-based access control, and includes a large collection of privileges that you can use to create a spectrum of roles. The privileges are described in the *vSphere Security* documentation. vSphere vCenter Server has nine roles defined. They vary in their functions and level of responsibility.

For this exercise, you create a role with a limited function: the ability to deploy new virtual machines from a template. A user with this role cannot move, modify, or delete a virtual machine, and cannot change the configuration of a host or datastore, for example. One scenario for this role is in an organization that provides virtual machine workstations to new hires, or needs to deploy development servers as new projects come on line. With a virtual machine deployment role in place, the manager can provide the role holder with a list of users and groups and needed virtual machines, and a runbook to follow for the process.

This chapter includes the following topics:

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 a 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 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.

Required Privileges for the Deploying a Virtual Machine Example

A set of privileges defines the limited role for a user whose only task is to deploy virtual machines from templates.

In this example of defining a limited role, you assign these privileges when you define the "Deployer of virtual machine from template" role in the Roles panel in the vSphere Client. See "Define the Role to Be Assigned in the Exercise," on page 89.

- **Datastore.Allocate space**
- **Datastore.Browse datastore**
- **Global.Cancel task**
- **Network.Assign network**
- **Resource.Assign virtual machine to resource pool**
- **Scheduled task.Create tasks**
- **Scheduled task.Run task**
- **Virtual machine.Configuration.Add new disk**
- **Virtual machine.Inventory.Create new**
- **Virtual machine.Provisioning.Deploy template**

Create and Configure a Role That Limits Users to Deploying Virtual Machines from Templates

For this example, the scenario is to create a role to be used by staff whose only function is to deploy virtual machines from templates as the need arises.

The steps in this exercise are based on the assumption that you already use a directory service like Microsoft Active Directory to administer users and groups for access to networked resources.

Use the information in Table 9-1 to enter values in the example steps for defining the role and for assigning permissions to it.

Table 9-1. Values to Use When Working with this Exercise

Item	Where Item Appears in the Interface	Value
Role **Name:**	In the **Roles** tab, select**Add Role**. In the **Permissions** tab, select the Assign Permissions dialog box and select the**Assigned Role** drop-down menu.	`Deployer of virtual machine from template`
Domain	In the **Permissions** tab, select the Assign Permissions dialog box, select the Select Users and Groups dialog box, and select the **Domain drop-down** menu.	*Domain of the directory service server that contains the names or groups you want to use in this exercise*
User **Name**	In the **Permissions** tab, select the Assign Permissions dialog box, the Select Users and Groups dialog box, and the Users and Groups pane.	*Name from your directory service*
Group **Name** (Optional)	In the **Permissions** tab, select the Assign Permissions dialog box, the Select Users and Groups dialog box, and the Users and Groups pane.	*Existing group in your directory service*

For information about roles and privileges, see the *vSphere Security* documentation.

Prerequisites

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

Verify the users and groups exist in your organization's directory service.

Procedure

1 Define the Role to Be Assigned in the Exercise on page 89

For the role exercise, you create and define the limited role in the vCenter Server by using the vSphere Client.

2 Assign Permissions on page 90

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.

What to do next

You can prepare a runbook for use by the staff with the role of deploying virtual machines.

Define the Role to Be Assigned in the Exercise

For the role exercise, you create and define the limited role in the vCenter Server by using the vSphere Client.

If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes that 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.

Access the list of privileges in "Required Privileges for the Deploying a Virtual Machine Example," on page 88.

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.

The name is **`Deployer of virtual machine from template`**.

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

The role **`Deployer of virtual machine from template`** is ready to be assigned to your selected user or group.

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.

Alarm Example: Setting an Alarm Action for Datastore Usage on a Disk 10

This example demonstrates a useful type of alarm action that you might configure for an object in the vSphere inventory, including responding to the alarm when it triggers.

Dozens of default alarm definitions are provided by the vSphere Client, which you can locate in the Alarms tab for an inventory object. One of these default alarms is **Datastore usage on disk**, which you use to monitor the percentage of disk usage. This kind of alarm is important if the virtual machines in the datastore have virtual disks in the thin provisioned format. With thin provisioning, at first a thin provisioned disk uses only as much datastore space as the disk initially needs. However, if the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

With thin provisioning, it is possible to oversubscribe storage space if the virtual machines grow unattended. An alarm set on the datastore can notify you when the space issues threaten to become critical.

This example demonstrates how to modify the **Datastore usage on disk** alarm to send emails when certain thresholds are reached.

NOTE VMware recommends that you first experiment with the procedures presented in *vSphere Examples and Scenarios* on test instances in your datacenter.

Required Privileges for Configuring and Acknowledging an Alarm

Someone who is assigned the Administrator role can configure alarms. Alarm privileges do not appear in other default sample roles accessible with the vSphere Client. To create a unique role for this process that does not include all the privileges of an Administrator, the following list contains the minimum privileges necessary.

- **Alarms.Create alarm**
- **Alarms.Modify alarm**
- **Alarms.Acknowledge alarm**

For information about roles, permissions, and privileges, see the *vSphere Security* documentation.

Configure and Act on an Alarm in a Scenario

Change alarm settings and specify what actions are taken when the alarm is triggered. Take ownership of an issue by acknowledging the alarm.

The Datastore usage on disk alarm is one of the many default alarms included with vCenter Server. The alarm is enabled at installation. If the used disk space on the datastore exceeds 75 percent, the alarm triggers a Warning. If the used disk space on the datastore then exceeds 85 percent, the alarm triggers an Alert. These warnings and alerts appear in the user interface in the form of modified icons for the elements affected. To have the alarm perform actions beyond this visual notification, change the configuration of the alarm. Follow the workflow in the sample tasks in this example scenario to become familiar with changing the settings of an alarm and responding to a triggered alarm.

Changes that you can make to this alarm are altering the percentage values for a Warning and for an Alert, modifying the frequency of an alarm, and defining the action the system takes at an alarm. For this example, you lower the percentage values, but keep the default frequency. In addition, on the **Actions** tab, you configure the action so that the system sends an email to specified addresses when a condition triggers the alarm. Use the values shown in Table 10-1 for making changes and configuring actions in the Alarm Settings dialog box.

Table 10-1. Values to Use in Changing the Settings of the Datastore Usage on Disk Alarm

Item	Where Item Appears in the Interface	Value
Alarm name, **Description**, **Alarm Type**	In the Alarm Settings dialog box, click the **General** tab.	Keep default.
Warning	In the Alarm Settings dialog box, click the **Triggers** tab.	**70**
Alert	In the Alarm Settings dialog box, click the **Triggers** tab.	**80**
Range, **Frequency**	In the Alarm Settings dialog box, click the **Reporting** tab.	Keep default.
Action > Add Action	In the Alarm Settings dialog box, click the **Action** tab.	**Send a notification email**
Configuration	In the Alarm Settings dialog box, click the **Action** tab.	*email_address_of_your_choice@your_organization.com*
From normal to warning	In the Alarm Settings dialog box, click the **Action** tab.	**Once**
From warning to alert	In the Alarm Settings dialog box, click the **Action** tab.	**Repeat**
From alert to warning	In the Alarm Settings dialog box, click the **Action** tab.	**Once**
From warning to normal	In the Alarm Settings dialog box, click the **Action** tab.	**Once**

In the procedures for acknowledging and resetting triggered alarms, follow the steps described in the vSphere Client option for both.

Procedure

1 Access Alarm Settings So You Can Make Changes in an Example Scenario on page 93

You can view alarm settings from any object, but you can modify settings only through the object on which the alarm is defined. You create and modify alarms in the Alarm Settings dialog box.

2 Specify How the Alarm is Triggered (Condition or State-based) on page 94

You can specify the events, states, or conditions that triggers the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

3 Specify Which Actions to Perform When Triggered on page 95

You can specify actions that the system performs when the alarm is triggered or changes status. You can enable and disable alarms and alarm actions independently of each other.

4 Acknowledge Triggered Alarms on page 96

Acknowledging an alarm lets other users know that you are taking ownership of the issue. After an alarm is acknowledged, its alarm actions are discontinued. For example, a host has an alarm set on it that monitors CPU usage and that sends an email to an administrator when the alarm is triggered. The host CPU usage spikes, triggering the alarm which sends an email to the host's administrator. The administrator acknowledges the triggered alarm to let other administrators know he is working on the problem, and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system. Alarms are neither cleared, nor reset when acknowledged.

5 (Optional) Reset Triggered Event Alarms on page 97

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.

Access Alarm Settings So You Can Make Changes in an Example Scenario

You can view alarm settings from any object, but you can modify settings only through the object on which the alarm is defined. You create and modify alarms in the Alarm Settings dialog box.

The default alarms are defined on the vCenter Server object.

Prerequisites

Verify that you have a vSphere Client connected to a vCenter Server.

Required privilege: **Alarm.Modify alarm**.

Procedure

1 In the vSphere Client, select the vCenter Server object on any inventory page.

2 Select the **Alarms** tab and click the **Definitions** tab.

3 Double-click **Datastore usage on disk**.

The Alarm Settings dialog box for the Datastore usage on disk alarm appears.

What to do next

Use the **Triggers** tab, the **Reporting** tab, and the **Action** tab to configure the alarm settings for the example scenario.

Specify How the Alarm is Triggered (Condition or State-based)

You can specify the events, states, or conditions that triggers the alarm in the Triggers tab of the Alarm Settings dialog box. The options you choose under the General tab of the Alarm Settings dialog box determine the options available under the Triggers tab. An alarm definition must contain at least one trigger before it can be saved.

Prerequisites

Open the Triggers tab of the Alarm Settings dialog box. See "View and Edit Alarm Settings," on page 94.

Required Privilege: **Alarms.Create Alarm** or **Alarm.Modify Alarm**

Procedure

1 Select the trigger you want to change or click **Add** to add a new trigger.

2 Click in the **Trigger Type** column and select an option from the drop-down menu.

3 Click in the **Condition** column and select an option from the drop-down menu.

4 Click in the **Warning** column and select an option from the drop-down menu to set the threshold for triggering a warning.

5 (Optional) Click in the **Condition Length** column and select an option from the drop-down menu.

6 Click in the **Alert** column and select an option from the drop-down menu to set the threshold for triggering an alert.

7 (Optional) Click in the **Condition Length** column and select an option from the drop-down menu.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or optionally add more triggers, or configure any of the following settings:for this alarm:

- Repeat alarm thresholds
- Repeat alarm frequency
- Alarm actions
- Alarm action frequency

View and Edit Alarm Settings

You create and modify alarms in the Alarm Settings dialog box. You can view alarm settings from any object, but you can modify settings only through the object on which the alarm is defined.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Required Privilege: **Alarms.Create Alarm** or **Alarm.Modify Alarm**

Procedure

- To view or change alarm settings, open the Alarm Settings dialog box:

Option	Description
Create New Alarm	Select an inventory object and select**File > New > Alarm**.
Add Alarm to Object	Right-click an inventory object and select **Alarm > Add Alarm**.
View Alarm Definitions	Select the **Alarms** tab, click the **Definitions** subtab of the inventory item with the alarm you want, and double-click an alarm in the list.

Specify Which Actions to Perform When Triggered

You can specify actions that the system performs when the alarm is triggered or changes status. You can enable and disable alarms and alarm actions independently of each other.

Prerequisites

Open the Actions tab of the Alarm Settings dialog box. See "View and Edit Alarm Settings," on page 94.

Ensure the vCenter Server is properly configured to use SNMP email or trap notifications as an alarm action.

Required Privilege: **Alarms.Create Alarm** or **Alarm.Modify Alarm**

Procedure

1. Select the action that you want to change or click **Add** to add one.
2. Click in the **Action** column and select an option from the drop-down menu.
3. Click in the **Configuration** column and enter configuration information for those actions that require additional information:

Option	Action
Send a notification email	Enter email addresses, separated by a comma, and press **Enter**.
Migrate a VM	Complete the Migrate Virtual Machine wizard .
Run a command	Take one of the following actions and press **Enter**: ■ If the command is a `.exe` file, enter the full path name of the command and include any parameters. For example, to run the `cmd.exe` command in the `C:\tools` directory, with the `alarmName` and `targetName` parameters, type: **`c:\tools\cmd.exe alarmName targetName`** ■ If the command is a `.bat` file, enter the full path name of the command as an argument to the `c:\windows\system32\cmd.exe` command. Include any parameters. For example, to run the `cmd.bat` command in the `C:\tools` directory, with the `alarmName` and `targetName` parameters, type: **`c:\windows\system32\cmd.exe /c c:\tools\cmd.bat alarmName targetName`** For `.bat` files, the command and its parameters must be formatted into one string.

4. (Optional) For each alarm status change column, specify whether the alarm should be triggered when the alarm status changes.

   Some actions do not support re-triggering on alarm status change.
5. For repeat actions, enter the time interval for the repetition in **Repeat After**.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

Send Email as an Alarm Action

You can use the SMTP agent included with vCenter Server to send email notifications when alarms are triggered.

Prerequisites

Ensure that the vCenter Server SMTP agent is properly configured to send email notifications.

Required Privilege: **Alarms.Create Alarm** or **Alarm.Modify Alarm**

Procedure

1 In the Actions tab of the Alarm Settings dialog box, click Add to add an action.

2 In the **Actions** column, select**Send a notification email** from the drop-down menu.

3 In the **Configuration** column, enter recipient addresses. Use commas to separate multiple addresses.

4 (Optional) Configure alarm transitions and frequency. See "Specify Which Actions to Perform When Triggered," on page 95.

What to do next

Click **OK** to save the alarm definition and exit the dialog box, or navigate to a different tab to make further changes.

Acknowledge Triggered Alarms

Acknowledging an alarm lets other users know that you are taking ownership of the issue. After an alarm is acknowledged, its alarm actions are discontinued. For example, a host has an alarm set on it that monitors CPU usage and that sends an email to an administrator when the alarm is triggered. The host CPU usage spikes, triggering the alarm which sends an email to the host's administrator. The administrator acknowledges the triggered alarm to let other administrators know he is working on the problem, and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system. Alarms are neither cleared, nor reset when acknowledged.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required privilege: **Alarm.Alarm Acknowledge**

Procedure

- Perform the following actions for the client you are using:

Option	Description
vSphere Client	a Display the inventory panel. b If necessary, select **View > Status Bar** to display the status pane. c In the status bar, click **Alarms** to display the Triggered Alarms panel. d Right-click the alarm and select **Acknowledge Alarm**. e To acknowledge multiple alarms at one time, shift-click each alarm to select it, right-click the selection, and select **Acknowledge Alarm**.
vSphere Web Client	a Select an inventory object. b Select **Monitor > Alarms**. c Select the alarms you want to acknowledge. Use Shift+Click or Ctrl+Click to select multiple alarms. d Click **Acknowledge**. Alternative methods: ■ Click **Acknowledge** in Alarm Details. ■ Right-click an alarm in the Alarm sidebar and select **Acknowledge**.

(Optional) Reset Triggered Event Alarms

An alarm triggered by an event might not reset to a normal state if vCenter Server does not retrieve the event that identifies the normal condition. In such cases, reset the alarm manually to return it to a normal state.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required privilege: **Alarm.Set Alarm Status**

Procedure

- Perform the following actions for the client you are using:

Option	Description
vSphere Client	a Locate the triggered alarm in the Triggered Alarms panel or on the **Alarms** tab for the object. b Right-click the alarm and select **Reset Alarm to Green**.
vSphere Web Client	a Select an inventory object. b Select **Monitor > Alarms**. c Select the alarms you want to reset. Use Shift+Click or Ctrl+Click to select multiple alarms. d Click **Reset to Green**. Alternative methods: ■ Click **Reset to green** in Alarm Details. ■ Right-click an alarm in the Alarm sidebar and select **Reset to green**.

Remediating Virtual Machines to Take Advantage of Enhancements to Virtual Hardware in vSphere 5.0

11

Remediation is the process in which VMware vSphere Update Manager applies patches, extensions, and upgrades to vSphere objects in groups. To take advantage of improvements in virtual hardware in vSphere 5.0, you can use Update Manager to update groups of virtual machines at one time.

The scenario in this example demonstrates the basic workflow for remediating virtual machines when virtual hardware upgrades become available.

Virtual Hardware Version and Remediation

All virtual machines have a hardware version. The hardware version indicates which virtual hardware features the virtual machine supports, such as BIOS or EFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics. The version of the ESXi host on which you have created the virtual machine determines the virtual machine hardware version.

vSphere 5.0 introduces hardware version 8. One example of added capability is that hardware version 8 supports up to 32 virtual CPUs instead of the previous number of 8 CPUs in hardware version 7. Although you might have updated your hosts with vSphere 5.0, the hardware version of the virtual machines is not automatically updated at that time. Without remediation, the virtual machines would continue to support only 8 CPUs.

Upgrading the virtual machines individually to hardware version 8 is tedious and inefficient. This is where remediation can help.

Remediation Path

The remediation path for applying the hardware upgrade to your virtual machines consists of choosing your baseline and baseline group, evaluating your virtual machines against that baseline, and upgrading the virtual machines to bring them into compliance with the configuration defined by the baseline.

By default, Update Manager takes snapshots of virtual machines before applying updates. If the remediation fails, you can use the snapshot to return the virtual machine to the state before the remediation.

Using Baselines and Baseline Groups

Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades. Update Manager has default upgrade baselines, one of which is **VM Hardware Upgrade to Match Host (Predefined)**, for checking the virtual hardware of a virtual machine for compliance with the latest version supported by the host.

To streamline the upgrade process even more, you can have Update Manager do an orchestrated upgrade of virtual machines, which includes the upgrade of VMware Tools through the **VMware Tools Upgrade to Match Host** baseline.

You assemble baseline groups from existing baselines. When you scan virtual machines, you evaluate them against baselines and baseline groups to determine their level of compliance.

Scanning Virtual Machines

Scanning is the process in which attributes of a set of hosts, virtual machines, or virtual appliances are evaluated against all patches, extensions, and upgrades in the attached baselines or baseline groups, depending on the type of scan you select. You can scan a virtual machine to determine whether it is up to date with the latest virtual hardware or VMware Tools version. When you select the **Virtual machine hardware upgrade scan**, you can scan virtual machines running Windows or Linux for the latest virtual hardware supported on the host. You can perform hardware-upgrade scans on online as well as offline virtual machines.

Remediating Virtual Machines

With remediation, Update Manager applies patches, extensions, and upgrades to hosts, virtual machines, or virtual appliances after a scan is complete. You can manually remediate virtual machines against baseline groups containing upgrade baselines.

For information about Update Manager and its functions, see the *Installing and Administering VMware vSphere Update Manager* documentation.

This chapter includes the following topics:

Update Manager Privileges

To configure Update Manager settings, to manage baselines, patches, and upgrades, you must have the proper privileges. You can assign Update Manager privileges to different roles from the vSphere Client.

Update Manager privileges cover distinct functionalities.

Table 11-1. Update Manager Privileges

Privilege Group	Privilege	Description
Configure	**Configure Service**	Configure the Update Manager service and the scheduled patch download task.
Manage Baseline	**Attach Baseline**	Attach baselines and baseline groups to objects in the vSphere inventory.
	Manage Baseline	Create, edit, or delete baseline and baseline groups.
Manage Patches and Upgrades	**Remediate to Apply Patches, Extensions, and Upgrades**	Remediate virtual machines, virtual appliances, and hosts to apply patches, extensions, or upgrades. In addition, this privilege allows you to view compliance status.
	Scan for Applicable Patches, Extensions, and Upgrades	Scan virtual machines, virtual appliances, and hosts to search for applicable patches, extensions, or upgrades.

Table 11-1. Update Manager Privileges (Continued)

Privilege Group	Privilege	Description
	Stage Patches and Extensions	Stage patches or extensions to hosts. In addition, this privilege allows you to view compliance status of the hosts.
	View Compliance Status	View baseline compliance information for an object in the vSphere inventory.
Upload File	**Upload File**	Upload upgrade images and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

Remediation Example: Remediate Virtual Machines When Virtual Hardware Upgrades Become Available

Use vSphere Update Manager to work with baselines and baseline groups, to scan virtual machines, and to upgrade those virtual machines with the new hardware version.

For this example, the scenario is to remediate virtual machines to upgrade their virtual hardware to version 8. As you go through the steps in this example, use the information in Table 11-2 to make entries and choices.

Table 11-2. Values to Use When Following the Remediation Example

Item	Where Item Appears in the Interface	Value
Baseline group	■ Click the**Baselines and Groups** tab and select**New Baseline Group**. ■ Select **Inventory** and click the **Update Manager** tab. Click the **Attach Update Manager** tab and select **Remediate**.	`Remediate VM Hardware`
Baselines to include in the group	Click the **Baselines and Groups** tab and select the **New Baseline Group**.	**VMware Tools Upgrade to Match Host** **VMware Hardware Upgrade to Match Host**
Type of object to attach to	Select **Inventory**.	**VMs and Templates**
Select an object	■ Select**Inventory**. ■ Click the **Update Manager** tab and select**Remediate**.	*The folder containing the targeted virtual machines*
Types of update to scan for	Select**Inventory > Scan for updates**.	**VMware Tools upgrades** **VM Hardware upgrades**

Prerequisites

You have installed VMware vSphere Update Manager and it is associated with a vCenter Server instance.

You have upgraded your hosts to vSphere 5.0

You have upgraded VMware Tools, if you are not performing an orchestrated upgrade.

You have collected the targeted virtual machines in a folder.

Remediation Example: Create a Baseline Group for the Remediation by Using Existing Baselines

The first task in the remediation path for this scenario is to create a baseline group using the predefined baselines for upgrading VMware Tools and for upgrading virtual machine hardware.

You assemble a baseline group from existing baselines. When you scan virtual machines you evaluate them against these baselines and baseline groups to determine the virtual machines' level of compliance.

For this scenario, look at the two predefined baselines that are used in an orchestrated upgrade of virtual machines. The two are VM Hardware Upgrade to Match Host, and VMware Tools Upgrade to Match Host.

Create a Virtual Machine and Virtual Appliance Baseline Group

You can combine upgrade baselines in a virtual machine and virtual appliance baseline group.

NOTE You can click **Finish** in the New Baseline Group wizard at any time to save your baseline group, and add baselines to it at a later stage.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baseline Groups pane.

2 In the New Baseline Group wizard, under Baseline Group Type, select **Virtual Machines and Virtual Appliances Baseline Group**.

3 Enter a name for the baseline group and click **Next**.

4 For each type of upgrade (virtual appliance, virtual hardware, and VMware Tools), select one of the available upgrade baselines to include in the baseline group.

NOTE If you decide to remediate only virtual appliances, the upgrades for virtual machines are ignored, and the reverse. If a folder contains both virtual machines and virtual appliances, the appropriate upgrades are applied to each type of object.

5 (Optional) Create a new Virtual Appliance upgrade baseline by clicking **Create a new Virtual Appliance Upgrade Baseline** at the bottom of the Upgrades page, and complete the New Baseline wizard.

After you complete the New Baseline wizard, you return to the New Baseline Group wizard.

6 Click **Next**.

7 On the Ready to Complete page, click **Finish**.

The new baseline group is displayed in the Baseline Groups pane.

Attach Baselines and Baseline Groups to Objects

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

You can attach baselines and baseline groups to objects from the Update Manager Client Compliance view.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and datacenters. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, you can attach baselines and baseline groups to objects managed by the vCenter Server system with which Update Manager is registered. Baselines and baseline groups you attach are specific for the Update Manager instance that is registered with the vCenter Server system.

Prerequisites

Ensure that you have the **Attach Baseline** privilege.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object that you want to attach the baseline to.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select the object in the inventory, and click the **Update Manager** tab.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, the **Update Manager** tab is available only for the vCenter Server system with which an Update Manager instance is registered.

4 Click **Attach** in the upper-right corner.

5 In the Attach Baseline or Group window, select one or more baselines or baseline groups to attach to the object.

If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.

6 (Optional) Click the **Create Baseline Group** or **Create Baseline** links to create a baseline group or a baseline and complete the remaining steps in the respective wizard.

7 Click **Attach**.

The baselines and baseline groups that you selected to attach are displayed in the Attached Baseline Groups and Attached Baselines panes of the **Update Manager** tab.

Remediation Example: Scan Virtual Machines and Review Compliance

The next task in the remediation path is to scan your virtual machines, and review them to determine whether they are up to date with the latest virtual hardware or VMware Tools version.

Manually Initiate a Scan of Virtual Machines and Virtual Appliances

To scan virtual machines and virtual appliances in the vSphere inventory immediately, you can manually initiate a scan against attached baselines and baseline groups.

Prerequisites

After you import a VMware Studio created virtual appliance in the vSphere Client, power it on so that it is discovered as a virtual appliance.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > VMs and Templates** in the navigation bar.

2 Right-click a virtual machine, virtual appliance, a folder of virtual machines and appliances, or a datacenter, and select **Scan for Updates**.

3 Select the types of updates to scan for.

The options are **Virtual Appliance upgrades**, **VM Hardware upgrades**, and **VMware Tools upgrades**.

4 Click **Scan**.

The virtual machines and appliances that you select are scanned against the attached baselines, depending on the options that you select. All child objects are also scanned. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes and the more accurate the compliance view is.

View Compliance Information for vSphere Objects

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

When you select a container object, you view the overall compliance status of the attached baselines, as well as all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object for which you want to view compliance information.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object from the inventory.

4 Click the **Update Manager** tab to view the scan results and compliance states.

Compliance View

Information about the compliance states of selected vSphere inventory objects against baselines and baseline groups you attach is displayed in the Update Manager Client Compliance view.

The information is displayed in four panes.

Table 11-3. Update Manager Tab Panes

Pane	Description
Attached Baseline Groups	Displays the baseline groups attached to the selected object. If you select **All Groups and Independent Baselines**, all attached baselines in the Attached Baselines pane are displayed. If you select an individual baseline group, only the baselines in that group are displayed in the Attached Baselines pane.
Attached Baselines	Displays the baselines attached to the selected object and included in the selected baseline group.

Table 11-3. Update Manager Tab Panes (Continued)

Pane	Description
Compliance	Contains a compliance graph that changes dynamically depending on the inventory object, baseline groups, and baselines that you select. The graph represents the percentage distribution of the virtual machines, appliances, or hosts in a selected container object that are in a particular compliance state against selected baselines. If you select an individual host, virtual machine, or appliance, the color of the graph is solid and represents a single compliance state. Above the graph, the following compliance states are displayed: **All Applicable** — Total number of inventory objects for which compliance is being calculated. This number is the total of objects in the selected container inventory object minus the objects for which the selected baselines are not applicable. The applicability of a baseline is determined on the basis of whether the baseline is directly attached to the virtual machine, appliance, or host, or whether it is attached to a container object. Applicability also depends on whether the baseline contains patches, extensions, or upgrades that can be applied to the selected object. **Non-Compliant** — Number of virtual machines, appliances, or hosts in the selected container object that are not compliant with at least one patch, extension, or upgrade in the selected baselines or baseline groups. **Incompatible** — Number of virtual machines, appliances, or hosts in the selected container object that cannot be remediated against the selected baselines and baseline groups. Incompatible state requires more attention and investigation for determining the reason for incompatibility. To obtain more information about the incompatibility, view patch, extension, or upgrade details. **Unknown** — Number of virtual machines, appliances, or hosts in the selected container object that are not scanned against at least one of the patches, extensions, or upgrades in the selected baselines and baseline groups. **Compliant** — Number of compliant virtual machines, appliances, or hosts in the selected container object.
Bottom pane	The information in this pane depends on whether you select an individual object or a container object. If you select a container object, the bottom pane of the **Update Manager** tab displays the following information: ■ A list of virtual machines, appliances, or hosts that meet the selections from the Attached Baseline Groups, Attached Baselines and Compliance panes. ■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups. If you select an individual object (such as virtual machine, appliance, or host), the bottom pane of the **Update Manager** tab displays the following information: ■ The number of patches, extensions, or upgrades included in the baseline or baseline group that you select. ■ The number of staged patches or extensions to a host. ■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups.

Table 11-3. Update Manager Tab Panes (Continued)

Pane	Description
	■ The vendor, product, version, compliance, release date as well as change log for the selected virtual appliance against the attached upgrade baseline.

Remediate Virtual Machines and Virtual Appliances

You can manually remediate virtual machines and virtual appliances immediately, or can schedule a remediation at a time that is convenient for you.

You can perform an orchestrated upgrade by using a virtual machine baseline group. The VMware Tools upgrade baseline runs first, followed by the virtual machine hardware upgrade baseline.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered. If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Home** page of the vSphere Client , select **VMs and Templates** and click the **Update Manager** tab.

2 Right-click a container object from the inventory and select **Remediate**.

All virtual machines and appliances in the container are also remediated.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and upgrade baselines to apply.

4 Select the virtual machines and appliances that you want to remediate and click **Next**.

5 On the Schedule page, specify a name and an optional description for the task.

6 Select **Immediately** to begin the remediation process immediately after you complete the wizard, or enter specific times for powered on, powered off, or suspended virtual machines.

7 (Optional) Choose whether to upgrade VMware Tools on power cycle.

This option is active only when you perform an upgrade against a single Upgrade VMware Tools to Match Host baseline. You can only enable VMware Tools upgrade on power cycle from the Remediate wizard, but you cannot disable it. You can disable the setting by clicking the **VMware Tools upgrade settings** button in the Update Manager Compliance view and deselecting the check box of a virtual machine in the Edit VMware Tools upgrade settings window.

8 (Optional) Specify the rollback options.

This option is not available if you selected to upgrade VMware Tools on power cycle.

a On the Rollback Options page of the Remediate wizard, select **Take a snapshot of the virtual machines before remediation to enable rollback**.

A snapshot of the virtual machine (or virtual appliance) is taken before remediation. If the virtual machine (or virtual appliance) needs to roll back, you can revert to this snapshot.

Update Manager does not take snapshots of fault tolerant virtual machines.

If you perform a VMware Tools upgrade and select to upgrade VMware Tools on power cycle, Update Manager takes no snapshots of the selected virtual machines before remediation.

b Specify when the snapshot should be deleted or select **Don't delete snapshots**.

c Enter a name and optionally a description for the snapshot.

d (Optional) Select the **Take a snapshot of the memory for the virtual machine** check box.

9 Click **Next**.

10 Review the Ready to Complete page, and click **Finish**.

Index

W