vSphere Upgrade

vSphere 5.0 Update 1

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

EN-000782-01

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 Upgrade 5

Updated Information 7

1 About the Upgrade Process 9

2 How vSphere 5.0 Differs from vSphere 4.x 11

3 System Requirements 13
- ESXi Hardware Requirements 13
- ESXi Support for 64-Bit Guest Operating Systems 16
- vCenter Server and vSphere Client Hardware Requirements 17
- vCenter Server Software Requirements 20
- vSphere Client and vSphere Web Client Software Requirements 21
- Providing Sufficient Space for System Logging 21
- Required Ports for vCenter Server 22
- Required Ports for the vCenter Server Appliance 23
- Conflict Between vCenter Server and IIS for Port 80 24
- DNS Requirements for vSphere 24
- Supported Remote Management Server Models and Minimum Firmware Versions 25
- Update Manager Hardware Requirements 25

4 Upgrading to vCenter Server 5.0 27
- Preparing for the Upgrade to vCenter Server 27
- Upgrade to vCenter Server 5.0 41
- Upgrade to vCenter Server on a Different Machine and Upgrade the Database 43
- Upgrade the VMware vCenter Server Appliance 58
- Update the VMware vCenter Server Appliance from a VMware.com Repository 58
- Update the VMware vCenter Server Appliance from a Zipped Update Bundle 59
- Update the VMware vCenter Server Appliance from the CD-ROM Drive 60
- vCenter Server Upgrade Fails When Unable to Stop Tomcat Service 60
- After You Upgrade vCenter Server 60

5 Upgrading Update Manager 71
- Upgrade the Update Manager Server 71
- Upgrade the Update Manager Client Plug-In 73

6 Upgrading and Migrating Your Hosts 75
- Preparing to Upgrade Hosts 75
- Performing the Upgrade or Migration 96
- After You Upgrade or Migrate Hosts 141

7 Upgrading Virtual Machines 143
About VMware Tools 144
About Virtual Machines and Host Upgrades 145
Virtual Machine Hardware Versions 146
Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager 147
Planning Downtime for Virtual Machines 152
Downtime for Upgrading Virtual Machines 152
Manually Install or Upgrade VMware Tools in a Windows Virtual Machine 153
Manually Install or Upgrade VMware Tools in a Linux Virtual Machine 154
Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine 156
Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine 157
Operating System Specific Packages for Linux Guest Operating Systems 158
Perform an Automatic Upgrade of VMware Tools 158
Upgrade VMware Tools on Multiple Virtual Machines 159
Configure a Virtual Machine to Upgrade VMware Tools Automatically 160
Upgrade Virtual Hardware 160
Upgrade Virtual Hardware on Multiple Virtual Machines 162
Uninstall VMware Tools 162

8 Example Upgrade Scenarios 165
Upgrading Environments with Host Clusters 165
Upgrading Environments Without Host Clusters 166
Moving Virtual Machines Using vMotion During an Upgrade 167
Moving Powered Off or Suspended Virtual Machines During an Upgrade with vCenter Server 168
Upgrading to vCenter Server on a New Machine 169
Migrating ESX 4.x or ESXi 4.x Hosts to ESXi 5.0 in a PXE-Booted Auto Deploy Installation 170
Upgrading vSphere Components Separately in a VMware View Environment 171

Index 173

About vSphere Upgrade

vSphere Upgrade describes how to upgrade or migrate to vSphere 5.0 Update 1.

To learn how to simplify and automate your datacenter upgrade, see the *vSphere Update Manager Installation and Administration Guide*.

If you have legacy versions of ESX, ESXi, and vCenter Server, and you want to move to VMware vSphere™ 5.0 Update 1 by performing fresh installations of vSphere components without preserving existing configurations, see the *vSphere Installation and Setup* documentation.

Intended Audience

vSphere Upgrade is for anyone who needs to upgrade from earlier versions of vSphere to vSphere 5.0 Update 1. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information

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

This table provides the update history of the *vSphere Upgrade*.

Revision	Description
000782-01	■ Updated entry for Oracle in Table: Table 4-2. ■ Corrected step 2 of procedure "Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script," on page 87.
000782-00	Initial release.

About the Upgrade Process 1

Upgrading is a multistage process in which procedures must be performed in a particular order. Follow theprocess outlined in this high-level overview to ensure a smooth upgrade with a minimum of system downtime.

CAUTION Make sure that you understand the entire upgrade process before you attempt to upgrade. If you do not follow the safeguards, you might lose data and lose access to your servers. Without planning, you might incur more downtime than is necessary.

You must complete the upgrade process in a specific order because you can lose data and server access. Order is also important within each upgrade stage.

You can perform the upgrade process for each component in only one direction. For example, after you upgrade to vCenter Server, you cannot revert to VirtualCenter 2.5. With backups and planning, you can restore your original software records.

You must complete one procedure before you move to the next procedure. Follow the directions within each procedure regarding the required sequence of minor substeps.

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you understand the irreversible changes at each stage before you upgrade your production environments.

To ensure that your datacenter upgrade goes smoothly, you can use vCenter Update Manager to manage the process for you.

vSphere upgrades proceed in the following sequence of tasks.

1. If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
2. If you are upgrading vSphere components that are part of a VMware View environment, see "Upgrading vSphere Components Separately in a VMware View Environment," on page 171.
3. Make sure your system meets vSphere hardware and software requirements.

   See Chapter 3, "System Requirements," on page 13.
4. If your vSphere deployment includes vCenter Server, upgrade vCenter Server.

   See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.
5. If you use VMware Update Manager, upgrade VMware Update Manager.

   See Chapter 5, "Upgrading Update Manager," on page 71.
6. Upgrade your ESXi hosts.

See Chapter 6, "Upgrading and Migrating Your Hosts," on page 75. vSphere 5.0.1 provides several ways to upgrade hosts:

- Use vSphere Update Manager to perform an orchestrated upgrade of your ESXi hosts. See "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 96.
- Upgrade a single host at a time, interactively, from an ESXi ISO installer image stored on a CD, DVD, or USB flash drive. See "Upgrade or Migrate Hosts Interactively," on page 110.
- Use a script to perform an unattended upgrade for multiple hosts. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 111
- If a host was deployed using vSphere Auto Deploy, you can use Auto Deploy to upgrade the host by reprovisioning it. See "Using vSphere Auto Deploy to Reprovision Hosts," on page 125.
- Patch ESXi 5.0 hosts from the using `esxcli` commands. See"Upgrading Hosts by Using esxcli Commands," on page 129.

7 Reapply your host license.

See "Reapplying Licenses After Upgrading to ESXi 5.0," on page 142.

8 Upgrade virtual machines and virtual appliances, manually or by using VMware Update Manager to perform an orchestrated upgrade.

See Chapter 7, "Upgrading Virtual Machines," on page 143.

How vSphere 5.0 Differs from vSphere 4.x

2

vSphere 5.0 is a major upgrade from vSphere 4.x.

The following changes from vSphere 4.x affect vSphere installation and setup. For a complete list of new features in vSphere 5.0, see the release notes.

Service Console is removed

ESXi does not include a Service Console. You can perform most tasks that you performed in the Service Console by using esxcli commands in the ESXi Shell, by using vCLI commands, and by using VMware PowerCLI commands. See *Command-Line Management in vSphere 5.0 for Service Console Users* and *Getting Started with vSphere Command-Line Interfaces*.

ESXi does not have a graphical installer

The graphical installer relied on the Service Console, which is not a part of ESXi. ESXi retains the text-based installer.

vSphere Auto Deploy and vSphere ESXi Image Builder CLI

Before ESXi 5.0, ESXi was installed on the physical disk of each ESXi host. With ESXi 5.0, you can load an ESXi image directly into memory by using vSphere Auto Deploy. You can provision and reprovision large numbers of ESXi hosts efficiently with vCenter Server, and manage ESXi updates and patching by using an image profile. You can save host configuration such as network or storage setup as a host profile and apply it to the host by using Auto Deploy. You can use ESXi Image Builder CLI to create ESXi installation images with a customized set of updates, patches, and drivers.

For complete information on using vSphere Auto Deploy and ESXi Image Builder PowerCLI, see the *vSphere Installation and Setup* documentation.

Changes in the ESXi installation and upgrade process

ESXi 5.0 uses a single installer wizard for fresh installations and upgrades. ESXi 5.0 also provides a new option for deploying ESXi directly into the host memory with vSphere Auto Deploy. The `vihostupdate` and `esxupdate` utilities are not supported for ESXi 5.0. You cannot upgrade or migrate to ESXi 5.0 by using any command-line utility. After you have upgraded or migrated to ESXi 5.0, you can upgrade or patch ESXi 5.0 hosts using vCLI `esxcli` commands.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

See "ESXi 5.0.x Upgrade and Update Options," on page 82.

Installer caching

Instead of using a binary image to install the system, whatever bits were used at boot time are cached to the system. This caching reduces installation problems caused by accessing installation files across networks that are under load.

NOTE Scripted installations cannot PXE boot a server and then obtain the binary image from some other form of media.

Changes to partitioning of host disks

All freshly installed hosts in vSphere 5.0 use the GUID Partition Table format instead of the MSDOS-style partition label. This change supports ESXi installation on disks larger than 2TB.

Newly installed vSphere 5.0 hosts use VMFS5, an updated version of the VMware File System for vSphere 5.0. Unlike earlier versions, ESXi 5.0 does not create VMFS partitions in second and successive disks.

Upgraded systems do not use GUID Partition Tables (GPT), but retain the older MSDOS-based partition label.

VMware vCenter Server Appliance

As an alternative to installing vCenter Server on a Windows machine, vSphere 5.0 provides the VMware vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

vSphere Web Client

The vSphere Web Client is a server application that provides a browser-based alternative to the traditional vSphere Client. You can use a Web browser to connect to the vSphere Web Client to manage an ESXi host through a vCenter Server.

System Requirements 3

Systems running vCenter Server and ESXi instances must meet specific hardware and operating system requirements.

If you are using Auto Deploy to provision ESXi hosts, see also the information about preparing for VMware Auto Deploy in the *vSphere Installation and Setup* documentation.

This chapter includes the following topics:

- "ESXi Hardware Requirements," on page 13
- "ESXi Support for 64-Bit Guest Operating Systems," on page 16
- "vCenter Server and vSphere Client Hardware Requirements," on page 17
- "vCenter Server Software Requirements," on page 20
- "vSphere Client and vSphere Web Client Software Requirements," on page 21
- "Providing Sufficient Space for System Logging," on page 21
- "Required Ports for vCenter Server," on page 22
- "Required Ports for the vCenter Server Appliance," on page 23
- "Conflict Between vCenter Server and IIS for Port 80," on page 24
- "DNS Requirements for vSphere," on page 24
- "Supported Remote Management Server Models and Minimum Firmware Versions," on page 25
- "Update Manager Hardware Requirements," on page 25

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.

To reconfigure `/scratch`, see the topic "Set the Scratch Partition from the vSphere Client" in the *vSphere Installation and Setup* documentation.

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.

Recommendation for Enhanced ESXi Performance

To enhance performance, install ESXi on a robust system with more RAM than the minimum required and with multiple physical disks.

For ESXi system requirements, see "ESXi Hardware Requirements," on page 13.

Table 3-1. Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. VMware recommends 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host. Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3GB of RAM for baseline performance. This figure includes approximately 1024MB for the virtual machines, 256MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines. These calculations do not take into account possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management* .
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS5 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. NOTE For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 5.0 drivers. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

ESXi Support for 64-Bit Guest Operating Systems

ESXi offers support for several 64-bit guest operating systems.

For a complete list of operating systems supported for ESXi, see the *VMware Compatibiity Guide* at http://www.vmware.com/resources/compatibility/search.php.

Hosts running virtual machines with 64-bit guest operating systems have the following hardware requirements:

- For AMD Opteron-based systems, the processors must be Opteron Rev E or later.

- For Intel Xeon-based systems, the processors must include support for Intel Virtualization Technology (VT). Many servers that include CPUs with VT support might have VT disabled by default, so you must enable VT manually. If your CPUs support VT ,but you do not see this option in the BIOS, contact your vendor to request a BIOS version that lets you enable VT support.

To determine whether your server has 64-bit VMware support, you can download the CPU Identification Utility from the VMware Web site.

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.
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.

VMware vCenter Server Appliance Hardware Requirements and Recommendations

IMPORTANT The embedded database is not configured to manage an inventory that contains more than 5 hosts and 50 virtual machines. If you use the embedded database with the vCenter Server Appliance, exceeding these limits can cause numerous problems, including causing vCenter Server to stop responding.

Table 3-4. Hardware Requirements for VMware vCenter Server Appliance

VMware vCenter Server Appliance Hardware	Requirement
Disk storage on the host machine	At least 7GB, and a maximum of 80GB
Memory in the VMware vCenter Server Appliance	■ Very small inventory (10 or fewer hosts, 100 or fewer virtual machines): at least 4GB. ■ Small inventory (10-100 hosts or 100-1000 virtual machines): at least 8GB. ■ Medium inventory (100-400 hosts or 1000-4000 virtual machines): at least 13GB. ■ Large inventory (More than 400 hosts or 4000 virtual machines): at least 17GB.

Table 3-5. Recommended JVM Heap Settings for VMware vCenter Server Appliance

vCenter Server Appliance 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

vSphere Client Hardware Requirements and Recommendations

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

Table 3-6. 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

vCenter Server and vSphere Client System Recommendations for Performance Based on Deployment Size

The number of hosts and powered-on virtual machines in your environment affects performance. Use the following system requirements as minimum guidelines for reasonable performance. For increased performance, you can configure systems in your environment with values greater than those listed here.

Processing requirements are listed in terms of hardware CPU cores. Only physical cores are counted. In hyperthreaded systems, logical CPUs do not count as separate cores.

IMPORTANT The recommended disk sizes assume default log levels. If you configure more detailed log levels, more disk space is required.

Table 3-7. Medium Deployment of Up to 50 Hosts and 500 Powered-On Virtual Machines

Product	Cores	Memory	Disk
vCenter Server	2	4GB	5GB
vSphere Client	1	1GB	1.5GB

Table 3-8. Large Deployment of Up to 300 Hosts and 3,000 Powered-On Virtual Machines

Product	Cores	Memory	Disk
vCenter Server	4	8GB	10GB
vSphere Client	1	1GB	1.5GB

Table 3-9. Extra-Large Deployment of Up to 1,000 Hosts and 10,000 Powered-On Virtual Machines

Product	Cores	Memory	Disk
vCenter Server	8	16GB	10GB
vSphere Client	2	1GB	1.5GB

vSphere Web Client Hardware Requirements

The vSphere Web Client has two components: A Java server and an Adobe Flex client application running in a browser.

Table 3-10. Hardware Requirements for the vSphere Web Client Server Component

vSphere Web Client Server Hardware	Requirement
Memory	At least 2GB: 1GB for the Java heap, and 1GB for ■ The resident code ■ The stack for Java threads ■ Global/bss segments for the Java process
CPU	2.00 GHz processor with 4 cores

Requirements for Installation of vCenter Server on a Custom Drive

If you install vCenter Server on a custom drive, note the following space requirements:

- 1GB on the custom drive for vCenter Server
- 1.13GB on the `C:\` drive for Microsoft .NET 3.0 SP1, Microsoft ADAM, Microsoft SQL Server 2008 R2 Express (optional), and Microsoft Visual C++ 2008 Redistributable
- 375MB for the custom drive `%temp%` directory

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.

The VMware vCenter Server Appliance can be deployed only on hosts that are running ESX version 4.x or ESXi version 4.x or later.

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.

Providing Sufficient Space for System Logging

ESXi 5.0 uses a new log infrastructure. If your host is deployed with Auto Deploy, or if you set up a log directory separate from the default location in a scratch directory on the VMFS volume, you might need to change your current log size and rotation settings to ensure that enough space for system logging exists.

All vSphere components use this infrastructure. The default values for log capacity in this infrastructure vary, depending on the amount of storage available and on how you have configured system logging. Hosts that are deployed with Auto Deploy store logs on a RAM disk, which means that the amount of space available for logs is small.

If your host is deployed with Auto Deploy, reconfigure your log storage in one of the following ways:

- Redirect logs over the network to a remote collector.
- Redirect logs to a NAS or NFS store.

You might also want to reconfigure log sizing and rotations for hosts that are installed to disk, if you redirect logs to nondefault storage, such as a NAS or NFS store.

You do not need to reconfigure log storage for ESXi hosts that use the default configuration, which stores logs in a scratch directory on the VMFS volume. For these hosts, ESXi 5.0 autoconfigures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 3-11. Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs.

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10240KB	10	100MB
VirtualCenter Agent (vpxa)	5120KB	10	50MB
vSphere HA agent (Fault Domain Manager, fdm)	5120KB	10	50MB

For information about setting up and configuring syslog and a syslog server, setting up syslog from the host profiles interface, and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

Required Ports for vCenter Server

The VMware vCenter Server system must be able to send data to every managed host and receive data from every vSphere Client. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other.

For information about ports required for the vCenter Server Appliance, see "Required Ports for the vCenter Server Appliance," on page 23.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from the vCenter Server system. If a firewall exists between any of these elements and Windows firewall service is in use, the installer opens the ports during the installation. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

NOTE In Microsoft Windows Server 2008, a firewall is enabled by default.

Table 3-12. Ports Required for Communication Between Components

Port	Description
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server. If you use a custom Microsoft SQL database (not the bundled SQL Server 2008 database) that is stored on the same host machine as the vCenter Server, port 80 is used by the SQL Reporting Service. When you install vCenter Server, the installer will prompt you to change the HTTP port for vCenter Server. Change the vCenter Server HTTP port to a custom value to ensure a successful installation. Microsoft Internet Information Services (IIS) also use port 80. See "Conflict Between vCenter Server and IIS for Port 80," on page 24.
389	This port must be open on the local and all remote instances of vCenter Server. This is the LDAP port number for the Directory Services for the vCenter Server group. The vCenter Server system needs to bind to port 389, even if you are not joining this vCenter Server instance to a Linked Mode group. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the LDAP service on any port from 1025 through 65535. If this instance is serving as the Microsoft Windows Active Directory, change the port number from 389 to an available port from 1025 through 65535.
443	The default port that the vCenter Server system uses to listen for connections from the vSphere Client. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. If you use another port number for HTTPS, you must use *ip-address*:*port* when you log in to the vCenter Server system.
636	For vCenter Server Linked Mode, this is the SSL port of the local instance. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the SSL service on any port from 1025 through 65535.
902	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts.
903	Port 903 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this ports to display virtual machine consoles.
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
60099	Web Service change service notification port
10443	vCenter Inventory Service HTTPS

Table 3-12. Ports Required for Communication Between Components (Continued)

Port	Description
10109	vCenter Inventory Service Management
10111	vCenter Inventory Service Linked Mode Communication

To have the vCenter Server system use a different port to receive vSphere Client data, see the *vCenter Server and Host Management* documentation.

For a discussion of firewall configuration, see the *vSphere Security* documentation.

Required Ports for the vCenter Server Appliance

The VMware vCenter Server system must be able to send data to every managed host and receive data from every vSphere Client. For migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other.

For information about ports required for vCenter Server on Windows, see "Required Ports for vCenter Server," on page 22.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from the vCenter Server system. The vCenter Server Appliance is preconfigured to use the ports listed in Table 3-13. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

Table 3-13. Ports Required for the vCenter Server Appliance

Port	Description
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server.
443	The default port that the vCenter Server system uses to listen for connections from the vSphere Client. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. If you use another port number for HTTPS, you must use *ip-address*:*port* when you log in to the vCenter Server system.
902	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts. Port 902 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this port to display virtual machine consoles.
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
10080	vCenter Inventory Service HTTP.
10443	vCenter Inventory Service HTTPS.
10109	vCenter Inventory Service database.
514	vSphere Syslog Collector server.
1514	vSphere Syslog Collector server (SSL).
6500	Network coredump server (UDP).
6501	Auto Deploy service.
6502	Auto Deploy management.
9090	vSphere Web Client HTTP.

Table 3-13. Ports Required for the vCenter Server Appliance (Continued)

Port	Description
9443	vSphere Web Client HTTPS.
5480	vCenter Server Appliance Web user interface HTTPS.
5489	vCenter Server Appliance Web user interface CIM service.
22	System port for SSHD.

To have the vCenter Server system use a different port to receive vSphere Client data, see the *vCenter Server and Host Management* documentation.

For a discussion of firewall configuration, see the *vSphere Security* documentation.

Conflict Between vCenter Server and IIS for Port 80

vCenter Server and Microsoft Internet Information Service (IIS) both use port 80 as the default port for direct HTTP connections. This conflict can cause vCenter Server to fail to restart after the installation of vSphere Authentication Proxy.

Problem

vCenter Server fails to restart after the installation of vSphere Authentication Proxy is complete.

Cause

If you do not have IIS installed when you install vSphere Authentication Proxy, the installer prompts you to install IIS. Because IIS uses port 80, which is the default port for vCenter Server direct HTTP connections, vCenter Server fails to restart after the installation of vSphere Authentication Proxy is complete. See "Required Ports for vCenter Server," on page 22.

Solution

- To resolve a conflict between IIS and vCenter Server for port 80, take one of the following actions.

Option	Description
If you installed IIS before installing vCenter Server	Change the port for vCenter Server direct HTTP connections from 80 to another value.
If you installed vCenter Server before installing IIS	Before restarting vCenter Server, change the binding port of the IIS default Web site from 80 to another value.

DNS Requirements for vSphere

You 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 and vSphere Web Clients. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Clients and vSphere Web Clients.

Ensure that the vCenter Server is installed on a machine that has a resolvable fully qualified domain name (FQDN). 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.

Ensure 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.

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 the 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.

Supported Remote Management Server Models and Minimum Firmware Versions

You can use remote management applications to install ESXi or for remote management of hosts.

Table 3-14. Supported Remote Management Server Models and Firmware Versions

Remote Controller Make and Model	Firmware Version	Java
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
IBM RSA 2	1.03, 1.2	1.6.0_22

Update Manager Hardware Requirements

You can run Update Manager on any system that meets the minimum hardware requirements.

Minimum hardware requirements for Update Manager vary depending on how Update Manager is deployed. If the database is installed on the same machine as Update Manager, requirements for memory size and processor speed are higher. To ensure acceptable performance, verify that your system meets the minimum hardware requirements.

Table 3-15. Minimum Hardware Requirements

Hardware	Requirements
Processor	Intel or AMD x86 processor with two or more logical cores, each with a speed of 2GHz
Network	10/100 Mbps
	For best performance, use a Gigabit connection between Update Manager and the ESX/ESXi hosts
Memory	2GB RAM if Update Manager and vCenter Server are on different machines
	4GB RAM if Update Manager and vCenter Server are on the same machine

Update Manager uses a SQL Server or Oracle database. You should use a dedicated database for Update Manager, not a database shared with vCenter Server, and should back up the database periodically. Best practice is to have the database on the same computer as Update Manager or on a computer in the local network.

Depending on the size of your deployment, Update Manager requires a minimum amount of free space per month for database usage. For more information about space requirements, see the *VMware vSphere Update Manager Sizing Estimator*.

For more information about ESXi 5.x and vCenter Server 5.x hardware requirements, see Chapter 3, "System Requirements," on page 13.

Supported Operating Systems and Database Formats

Update Manager works with specific databases and operating systems.

The Update Manager server requires a 64-bit Windows system.

NOTE Make sure the system on which you are installing Update Manager server is not an Active Directory domain controller.

The Update Manager plug-in requires the vSphere Client, and works with the same operating systems as the vSphere Client.

Update Manager scans and remediates Windows and Linux virtual machines for VMware Tools and virtual hardware upgrades.

The Update Manager server requires SQL Server or Oracle database. Update Manager can handle small-scale environments using the bundled SQL Server 2008 R2 Express. For environments with more than 5 hosts and 50 virtual machines, create either an Oracle or a SQL Server database for Update Manager. For large scale environments, you should set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database.

For detailed information about supported operating systems and database formats, see the *vSphere Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

For detailed information about supported database formats, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Upgrading to vCenter Server 5.0

4

The upgrade to vCenter Server includes a database schema upgrade and an upgrade of vCenter Server 4.x.

This chapter includes the following topics:

- "Preparing for the Upgrade to vCenter Server," on page 27
- "Upgrade to vCenter Server 5.0," on page 41
- "Upgrade to vCenter Server on a Different Machine and Upgrade the Database," on page 43
- "Upgrade the VMware vCenter Server Appliance," on page 58
- "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 58
- "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 59
- "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 60
- "vCenter Server Upgrade Fails When Unable to Stop Tomcat Service," on page 60
- "After You Upgrade vCenter Server," on page 60

Preparing for the Upgrade to vCenter Server

Before you upgrade to vCenter Server, make sure your system is properly prepared.

See "Best Practices for vCenter Server Upgrades," on page 29.

About the vCenter Server 5.0.x Upgrade

VMware supports in-place upgrades on 64-bit systems from vCenter Server 4.x and vCenter Server 5.0 to vCenter Server 5.0.x.

You can upgrade VirtualCenter 2.5 Update 6 or later and vCenter Server 4.0.x to vCenter Server 5.0.x by installing vCenter Server 5.0.x on a new machine and migrating the existing database. This upgrade method makes it possible to upgrade from a 32-bit system to a 64-bit system. Alternatively, if the VirtualCenter or vCenter Server database is on a remote machine, you can upgrade the database.

vCenter Server 5.0.x can manage ESX 3.5.x/ESXi 3.5.x hosts in the same cluster with ESX 4.x/ESXi 4.x hosts.

NOTE You cannot upgrade a vCenter Server 4.x instance that is running on Windows XP Professional x64 Edition to vCenter Server 5.0, because vCenter Server 5.0.x does not support Windows XP Professional x64.

vCenter Server Upgrade Summary

The upgrade to vCenter Server 5.0.x affects other software components of your datacenter.

Table 4-1 summarizes the effect on your datacenter components.

Table 4-1. Upgrading vCenter Server Components

Product	Component	Description
vCenter Server, vSphere Client, and vSphere Web Client	VI Client 1.x	Not supported.
	VirtualCenter Server 1.x	Not supported.
	VirtualCenter Server 2.0	Not supported.
	VirtualCenter Server 2.5	Not supported.
	VirtualCenter Server 2.5 Update 6	Upgrade by using the data migration tool to upgrade to vCenter Server 5.0.x on a different machine. Alternatively, if the VirtualCenter database is on a remote machine, you can simply upgrade the database.
	vCenter Server 4.0	Upgrade in place if it is installed on a 64-bit system. If it is installed on a 32-bit system, upgrade by using the data migration tool to upgrade to vCenter Server 5.0.x on a different machine.
	vSphere Client 4.0	Not supported.
	vCenter Server 4.1	In place upgrade.
	vSphere Client 4.1	Not supported.
	vCenter Server 5.0	Upgrade to vCenter Server 5.0.x.
	vCenter Client 5.0	Upgrade to vCenter Client 5.0.x.
	vSphere Web Client 5.0	Upgrade to vSphere Web Client 5.0.x.
	IBM DB2 database	Verify that your database is supported. Upgrade if necessary.
	Oracle database	Verify that your database is supported. Upgrade if necessary. Oracle 9i is no longer supported.
	SQL database	Verify that your database is supported. Upgrade if necessary. Microsoft SQL Server 2000 is no longer supported. Microsoft SQL Server 2008 Express is supported in vCenter Server 5.0.x
	Linked Mode	You cannot join a vCenter Server to a Linked Mode group during the upgrade procedure. Join after the upgrade to vCenter Server is complete. If you are upgrading a version 5.0 vCenter Server that is part of a Linked Mode group, it will not be removed from the group. If you are upgrading a pre-5.0 vCenter Server that is part of a Linked Mode group, it will be removed from the group. vCenter Server does not support Linked Mode groups that contain both version 5.0.x and pre-5.0 versions of vCenter Server. After all vCenter Servers in the group are upgraded to version 5.0.x, you can rejoin them.
License server	License server	To manage ESX 3.5x/ESXi 3.5 hosts, verify that the vCenter Server system is configured to use a license server. Install a license server if necessary.
ESX and ESXi	ESX 2.5 host	Not supported with vCenter Server 5.0.x
	VMFS2 volumes	Supported as read-only (deprecated).
	VM2 virtual machines	Upgrade (optional).
	VMDK2 virtual disk	Not supported with vCenter Server 5.0.x
	ESX MUI	No change.
	VMware Tools	Upgrade (optional).
	ESX/ESXi 3.5 host	Upgrade to ESXi 5.0.x (optional).
	ESX/ESXi 4.0 host	Upgrade to ESXi 5.0.x (optional)

Table 4-1. Upgrading vCenter Server Components (Continued)

Product	Component	Description
	ESX/ESXi 4.1 host	Update to 4.1 Update 1 or later before upgrading vCenter Server to version 5.0 (required). Upgrade to ESXi 5.0.x (optional).
	ESXi 5.0 host	Upgrade to ESXi 5.0.x (optional).
	VMFS3 volumes	No change.
	VM3 virtual machines	Upgrade (optional).
	VMDK3 virtual disk	Not supported with vCenter Server 5.0.

Best Practices for vCenter Server Upgrades

When you upgrade vCenter Server, you must understand and follow the best practices process for a successful upgrade.

To ensure that each upgrade is successful, follow these best practices:

1 Make sure that you understand the vCenter Server upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.

- If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Read all the subtopics in "Preparing for the Upgrade to vCenter Server," on page 27.
- Read the VMware vSphere 5.0 Release Notes for known installation issues.
- If your vSphere installation is in a VMware View environment, see "Upgrading vSphere Components Separately in a VMware View Environment," on page 171.

2 Prepare your system for the upgrade.

- Make sure your system meets requirements for vCenter Server 5.0. See Chapter 3, "System Requirements," on page 13 and the VMware Compatibility Guide, at http://www.vmware.com/resources/compatibility/search.php.
- Verify that your existing database is supported for vCenter Server 5.0. See "vCenter Server Database Patch and Configuration Requirements," on page 33 and the VMware Compatibility Guide, at http://www.vmware.com/resources/compatibility/search.php.
- Make sure that your vCenter Server database is prepared and permissions are correctly set. See the information about preparing vCenter server databases in the *vSphere Installation and Setup* documentation.
- Review the prerequisites for the upgrade. See "Prerequisites for the vCenter Server Upgrade," on page 30.

3 Back up your vCenter Server databases and SSL certificates

- Make a full backup of the vCenter Server database and the vCenter Inventory Service database. For the vCenter Server database, see the vendor documentation for your vCenter Server database type. For the Inventory Service database, see the topics "Back Up the Inventory Service Database on Windows" and "Back Up the Inventory Service Database on Linux" in the *vSphere Installation and Setup* documentation.
- Back up the SSL certificates that are on the VirtualCenter or vCenter Server system before you upgrade to vCenter Server 5.0. The default location of the SSL certificates is `%allusersprofile%\Application Data\VMware\VMware VirtualCenter`. See "Back Up VirtualCenter 2.5 Update 6 or Higher," on page 35.

4 Stop the VMware VirtualCenter Server service.

5 Run the vCenter Host Agent Pre-Upgrade Checker, and resolve any issues that the Pre-Upgrade Checker finds. See"Run the vCenter Host Agent Pre-Upgrade Checker," on page 36.

6 Make sure that no processes are running that conflict with the ports that vCenter Server uses. See "Required Ports for vCenter Server," on page 22.

7 Run the vCenter Server upgrade.

8 Configure new vSphere 5.0 licenses.

9 Upgrade the vSphere Client to version 5.0 to prevent compatibility problems that can interfere with the operation of the vSphere Client. See "Upgrade the vSphere Client," on page 61.

10 Review the topics in "After You Upgrade vCenter Server," on page 60 for post-upgrade requirements and options.

Prerequisites for the vCenter Server Upgrade

Before you begin the upgrade to vCenter Server, make sure you prepare the vCenter Server system and the database.

vCenter Server Prerequisites

The following items are prerequisites for completing the upgrade to vCenter Server:

- VMware vCenter Server 5.0 installation media.
- License keys for all purchased functionality.

  If you do not have the license key, you can install in evaluation mode and use the vSphere Client to enter the license key later. If the vCenter Server that you are upgrading is in evaluation mode, after the upgrade, the time remaining in your evaluation period is decreased by the amount already used. For example, if you used 20 days of the evaluation period before upgrading, your remaining evaluation period after the upgrade is 40 days.

  If you do not intend to use evaluation mode, make sure that you have new license keys during an upgrade. Old license keys are not supported in vCenter Server 5.0.
- The installation path of the previous version 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 your previous version of vCenter Server does not meet this requirement, you must perform a clean installation of vCenter Server 5.0.
- Make sure the system on which you are installing vCenter Server is not an Active Directory primary or backup domain controller.
- Either remove any ESX Server 2.x hosts from the VirtualCenter or vCenter Server inventory or upgrade these hosts to 3.5 or later.
- If you are upgrading to vCenter Server 5.0, update any ESX/ESXi 4.1 hosts to version 4.1 Update 1 or later. See Knowledge Base article 2009586.
- Make sure that the computer name has 15 characters or fewer.
- Run the vCenter Host Agent Pre-Upgrade Checker.
- Make sure that SSL certificate checking is enabled for all vSphere HA clusters. If certificate checking is not enabled when you upgrade, HA will fail to configure on the hosts.
  - In vCenter Server 4.x, select **Administration > vCenter Server Settings > SSL Settings > vCenter requires verified host SSL certificates**. Follow the instructions to verify each host SSL certificate and click **OK**.

  - In VirtualCenter 2.5 Update 6 or later, select **Administration > Virtual Center Management Server Configuration > SSL Settings > Check host certificates** and click **OK**. When you enable SSL checking in VirtualCenter 2.5, the hosts are disconnected from vCenter Server, and you must reconnect them.

- If the vCenter Server 4.x environment that you are upgrading includes Guided Consolidation 4.x, uninstall Guided Consolidation before upgrading to vCenter Server 5.0.
- If you use vCenter Guided Consolidation Service in the VirtualCenter 2.x environment, complete the consolidation plan before you upgrade to vCenter Server 5.0. The upgrade to vCenter Server 5.0 does not preserve or migrate any data gathered by the vCenter Guided Consolidation Service. After the upgrade, all of the data is cleared, and you cannot restore it.
- Back up the SSL certificates that are on the VirtualCenter or vCenter Server system before you upgrade to vCenter Server 5.0. The default location of the SSL certificates is `%allusersprofile%\Application Data\VMware\VMware VirtualCenter`.
- vCenter Server 5.0 uses TCP/IP Ports 80 and 443 for the VMware vSphere Web client. You cannot run vCenter Server on the same machine as a Web server using TCP/IP port 80 (HTTP) or port 443 (HTTPS) because doing so causes port conflicts.
- Verify that the fully qualified domain name (FQDN) of the system where you will upgrade 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 upgrade 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.
- If you use DHCP instead of a manually assigned (static) IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Test this is by pinging the computer name. 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.
- 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.

Prerequisites for All vCenter Server Databases

- If your database server is not supported by vCenter Server, perform a database upgrade to a supported version or import your database into a supported version. See "Supported Database Upgrades," on page 34.
- Perform a complete backup of the VirtualCenter Server or vCenter Server database before you begin the upgrade. The VirtualCenter 2.5 database schema is not compatible with vCenter Server 5.0. The vCenter Server 5.0 installer upgrades your existing VirtualCenter Server database schema with extra fields, making the database unusable by VirtualCenter 2.5 Update 6.

  To remove the DBO role, you can migrate all objects in the DBO schema to a custom schema. See the VMware knowledge base article at http://kb.vmware.com/kb/1036331.
- You must have login credentials, the database name, and the database server name that will be used by the vCenter Server database. The database server name is typically the ODBC System database source name (DSN) connection name for the vCenter Server database.

- Review "Supported Database Upgrades," on page 34.

Prerequisites for Microsoft SQL Databases

- To use a newly supported Microsoft SQL database, such as Microsoft SQL 2008, you do not need to perform a clean installation of vCenter Server if your existing database is also Microsoft SQL Server. For example, you can upgrade a Microsoft SQL Server 2000 database to Microsoft SQL Server 2005 or Microsoft SQL Server 2008 and then upgrade VirtualCenter 2.5 Update 6 or higher to vCenter Server 5.0. When you migrate the database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or higher, set the compatibility level of the database to 90.
- JDK 1.6 must be installed on the vCenter Server machine. In addition, `sqljdbc4.jar` must be added to the CLASSPATH variable on the machine where vCenter Server is to be upgraded. If it is not installed on your system, the vCenterServer installer installs it. The JDK 1.6 installation might require Internet connectivity.
- If you are upgrading from VirtualCenter 2.5 Update 6 with the bundled SQL Server 2005 Express (by installing vCenter Server 5.0 on a different machine and keeping the database), you do not have to perform a clean installation of vCenter Server.
- Your system DSN must be using the SQL Native Client driver.
- Grant the following permissions to the vCenter user in the vCenter database:

```
GRANT ALTER ON SCHEMA :: <schema> to <user>;
GRANT REFERENCES ON SCHEMA :: <schema> to <user>;
GRANT INSERT ON SCHEMA :: <schema>  to <user>;
GRANT CREATE TABLE to <user>;
GRANT CREATE VIEW to <user>;
GRANT CREATE Procedure to <user>;
```

  Grant the following permissions to the user in the MSDB database:

```
GRANT SELECT on msdb.dbo.syscategories to <user>;
GRANT SELECT on msdb.dbo.sysjobsteps to <user>;
GRANT SELECT ON msdb.dbo.sysjobs to <user>;
GRANT EXECUTE ON msdb.dbo.sp_add_job TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_update_job TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_add_category TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO <user>;
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO <user>;
```

Prerequisites for Oracle Databases

- To use a newly supported Oracle database, such as Oracle 11g, you do not need to perform a clean installation of vCenter Server if your existing database is also Oracle. For example, you can upgrade your existing Oracle 9i database to Oracle 10g or Oracle 11g and then upgrade vCenter Server 4.x to vCenter Server 5.0.
- The JDBC driver file must be included in the CLASSPATH variable.
- Either assign the DBA role or grant the following permissions to the user:

```
grant connect to <user>
grant resource to <user>
grant create view to <user>
grant create any sequence to <user>
grant create any table to <user>
```

```
grant create materialized view to <user>
grant execute on dbms_job to <user>
grant execute on dbms_lock to <user>
grant unlimited tablespace to <user> # To ensure sufficient space
```

After the upgrade is complete, you can optionally remove the following permissions from the user profile: **create any sequence** and **create any table**.

By default, the **RESOURCE** role has the **CREATE PROCEDURE**, **CREATE TABLE**, and **CREATE SEQUENCE** privileges assigned. If the **RESOURCE** role lacks these privileges, grant them to the vCenter Server database user.

Prerequisite for IBM DB2 Databases

To use a newly supported IBM DB2 database, you must use vCenter Server 4.0 Update 1 or higher. Previous releases of VirtualCenter or vCenter Server do not support DB2 databases.

vCenter Server Database Patch and Configuration Requirements

After you choose a database type, make sure you understand the configuration and patch requirements for the database.

NOTE vCenter Update Manager also requires a database. VMware recommends that you use separate databases for vCenter Server and vCenter Update Manager.

vCenter Server databases require a UTF code set.

If your VirtualCenter 2.5 Update 6 database is not supported for upgrade to vCenter Server 5, first upgrade your database and then upgrade to vCenter Server. You also can import your database into a database that is supported for upgrade to vCenter Server.

If your database is not listed in Table 4-2, see "Supported Database Upgrades," on page 34.

For information about specific database versions and service pack configurations supported with vCenter Server, see the VMware Product Interoperability Matrixes.

Table 4-2. Configuration Notes for Databases Supported with vCenter Server

Database Type	Configuration Notes
IBM DB2	If the database is not local to the vCenter Server system, install the IBM Data Server Runtime Client. Install the IBM DB2 native client according to the IBM instructions for your DB2 version. Ensure that the DB2 binaries directory (typically `C:\Program Files\IBM\SQLLIB\BIN`) is in the system path. DB2 might be installed at a different location. You might need to restart the Microsoft Windows machine for the service to recognize the change in the environment variable. Ensure that the machine has a valid ODBC data source name (DSN) entry. **NOTE** This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2008 R2 Express	Bundled database that you can use for small deployments of up to 5 hosts and 50 virtual machines. You cannot install the bundled database during an upgrade to vCenter Server. To use the bundled database, Microsoft SQL Server 2008 R2 Express must be already installed or you must perform a clean installation of vCenter Server. **NOTE** This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2005	Ensure that the machine has a valid ODBC DSN entry. **NOTE** This database is not supported for the vCenter Server Appliance.

Table 4-2. Configuration Notes for Databases Supported with vCenter Server (Continued)

Database Type	Configuration Notes
Microsoft SQL Server 2008	Ensure that the machine has a valid ODBC DSN entry. NOTE This database is not supported for the vCenter Server Appliance.
Oracle	For Oracle 10g R2, if necessary, first apply patch 10.2.0.4 (or later) to the client and server. You can then apply patch 5699495 to the client. Ensure that the machine has a valid ODBC DSN entry. After you complete the vCenter Server installation, take the following steps: ■ Apply the latest patch to the Oracle client and server. ■ Copy the Oracle JDBC driver (ojdbc14.jar or ojdbc5.jar) to the vCenter Server installation directory, in the `tomcat\lib` subdirectory: *`vCenter install location`*`\Infrastructure\tomcat\lib`. The vCenter Server installer attempts to copy the Oracle JDBC driver from the Oracle client location to the vCenter Server installation directory. If the Oracle JDBC driver is not found in the Oracle client location, the vCenter Server installer prompts you to copy the file manually. You can download the file from the oracle.com Web site.

Supported Database Upgrades

When you upgrade, migrate, or update to vCenter Server 5.0 or 5.0.1, make sure that the upgraded version supports your database.

Table 4-3 lists the database types that you can use with vCenter Server 5.0 or 5.0.1. The purpose of this list is to describe the vCenter Server Upgrade scenarios for each database type. For a list of supported database versions, See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Table 4-3. vCenter Server Upgrade, Migration, or Update Scenarios for Each Database Type

Database Type	Supported in vCenter Server 5.0.x	Supported Upgrade, Migration, or Update
IBM DB2 9.5	Yes	You can upgrade to vCenter Server 5.0.x from vCenter Server 4.0 Update 1, vCenter Server 4.0 Update 2, vCenter Server 4.1, and update to vCenter Server 5.0.x from vCenter Server 5.0. You cannot upgrade from vCenter Server 4.0 because vCenter Server 4.0 Update 1 is the first release that supports IBM DB2 database servers.
IBM DB2 9.7	Yes	You can upgrade to vCenter Server 5.0.x from vCenter Server 4.0 Update 3, vCenter Server 4.1 Update 1, and update to vCenter Server 5.0.x from vCenter Server 5.0.
Experimental MSDE database	No	After you upgrade to a database server that is supported by vCenter Server, you can install or upgrade to vCenter Server 5.0.x.
MS SQL Server 2000	No	After you upgrade to a database server that is supported by vCenter Server, you can install, upgrade, or update to vCenter Server.
MS SQL Server 2005 Express	No	After you upgrade to a database server that is supported by vCenter Server, you can install, upgrade, or update to vCenter Server.
MS SQL Server 2005	Yes	You can install, upgrade, or update to vCenter Server.
MS SQL Server 2008 Express	Yes.	You can perform a fresh installation of vCenter Server 5.0 or update to vCenter Server 5.0.x. You cannot upgrade from vCenter Server versions earlier than 5.0 because vCenter Server 5.0 is the first release that supports Microsoft SQL Server 2008 Express.
MS SQL Server 2008	Yes	You can install, upgrade, or update to vCenter Server 5.0.x.
Oracle 9i	No	After you upgrade to a database server that is supported by vCenter Server, you can install, upgrade, or update to vCenter Server 5.0.x.

Table 4-3. vCenter Server Upgrade, Migration, or Update Scenarios for Each Database Type (Continued)

Database Type	Supported in vCenter Server 5.0.x	Supported Upgrade, Migration, or Update
Oracle 10g	Yes	You can install, upgrade, or update to vCenter Server 5.0.x.
Oracle 11g	Yes	You can install, upgrade, or update to vCenter Server 5.0.x.

Configure vCenter Server to Communicate with the Local Database

The machine on which you install or upgrade to vCenter Server must have a computer name that is 15 characters or fewer. If your database is located on the same machine on which vCenter Server will be installed, and you have recently changed the name of this machine to comply with the name-length requirement, make sure the vCenter Server DSN is configured to communicate with the new name of the machine.

Changing the vCenter Server computer name impacts database communication if the database server is on the same computer with vCenter Server. If you changed the machine name, you can verify that communication remains intact.

The name change has no effect on communication with remote databases. You can skip this procedure if your database is remote.

NOTE The name-length limitation applies to the vCenter Server system. The data source name (DSN) and remote database systems can have names with more than 15 characters.

Check with your database administrator or the database vendor to make sure all components of the database are working after you rename the server.

Prerequisites

- Make sure the database server is running.
- 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.

Procedure

1 Update the data source information, as needed.

2 Verify the data source connectivity.

Back Up VirtualCenter 2.5 Update 6 or Higher

You must back up a VirtualCenter system to ensure that you can restore your previous configuration of VirtualCenter if the upgrade does not complete successfully. The only way to recover from an unsuccessful upgrade is to use your backed up database and SSL certificates.

You cannot roll back your database to the previous database schema.

Procedure

1 Make a full backup of the VirtualCenter 2.5 Update 6 or higher database.

  See your database documentation.

2 Back up the VirtualCenter 2.5 Update 6 or higher SSL certificates.

   a Copy the SSL certificate folder under `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter`.

   b Paste it at the backup location.

3 Take notes on the existing VirtualCenter installation regarding the selections, settings, and information used.

   For example, note any nondefault settings, such as the IP address, the database DSN, user name, password, and assigned ports.

4 Create a backup copy of `vpxd.cfg`.

What to do next

Continue with the upgrade to vCenter Server.

About the vCenter Host Agent Pre-Upgrade Checker

The vCenter Host Agent Pre-Upgrade Checker produces a report showing known issues that might prevent a successful upgrade of the vCenter Host Agent software.

To ensure a successful upgrade to vCenter Server 5, you must diagnose and fix any potential problems on the managed ESX/ESXi hosts. You can run the vCenter Host Agent Pre-Upgrade Checker for in-place upgrades from vCenter Server 4.x to vCenter Server 5.0.

vCenter Host Agent runs on all managed ESX/ESXi hosts. This software coordinates actions received from vCenter Server. When you add a host to vCenter Server, the agent is installed on the physical ESX/ESXi host. When you upgrade to vCenter Server 5, the agent residing on each ESX/ESXi host must be upgraded as well.

During a vCenter Server upgrade, the existing agent software is uninstalled and the updated agent software is installed in its place. If the upgrade fails, the updated agent software might not be installed and the host might become unreachable by VirtualCenter 2.5 Update 6 or later, vCenter Server 4.x, or by vCenter Server 5.0. To avoid this condition, you can run the vCenter Host Agent Pre-Upgrade Checker before you try to upgrade to vCenter Server 5.

The vCenter Host Agent Pre-Upgrade Checker checks to make sure that the agent software is ready to be upgraded. Some of the checks include checking to make sure that the host is reachable, the disk space is sufficient, the network is functioning, the file system is intact, and required patches are applied. Each time you run the tool, the system queries VMware.com and downloads any new updates for the tool. This action ensures that as new upgrade issues are discovered, the tool remains as useful as possible.

Important A successful vCenter Host Agent pre-upgrade check does not guarantee a successful upgrade to vCenter Server 5. An upgrade to vCenter Server involves multiple components, and the tool checks only one component: the vCenter Host Agent. Also, the tool checks only known issues. Other issues might be present that the tool does not check.

The vCenter Host Agent Pre-Upgrade Checker does not fix the reported issues. You must resolve the reported issues manually and rerun the tool to verify that the issues are resolved.

For the procedure to run the vCenter Host Agent Pre-Upgrade Checker, see "Run the vCenter Host Agent Pre-Upgrade Checker," on page 36.

Run the vCenter Host Agent Pre-Upgrade Checker

The vCenter Host Agent Pre-Upgrade Checker reports known issues that might prevent a successful upgrade of the vCenter Host Agent software.

For more information about the vCenter Host Agent Pre-Upgrade Checker, see "About the vCenter Host Agent Pre-Upgrade Checker," on page 36.

Prerequisites

- Verify that VirtualCenter 2.5 Update 6 or later or vCenter Server is installed on a Windows machine that is supported by vCenter Server 5.
- Verify that the VirtualCenter 2.5 Update 6 or vCenter Server machine has a DSN configured that is compatible with vCenter Server 5.
- Verify that the VirtualCenter 2.5 Update 6 or vCenter Server database is supported by vCenter Server 5. If necessary, upgrade the database to work with vCenter Server 5. The MSDE database was supported in experimental mode in VirtualCenter Server 2.0.x, but is not supported in vCenter Server 5. The vCenter Host Agent Pre-Upgrade Checker will not detect the database. Upgrade to a supported database before using the tool. See "Supported Database Upgrades," on page 34.
- Verify that the ESX/ESXi hosts are managed by VirtualCenter 2.5 Update 6 or later or by vCenter Server.
- Verify that VirtualCenter Agent or vCenter Host Agent software is running on each managed ESX/ESXi host.
- Verify that Microsoft .NET Framework Version 2.0 is installed on the VirtualCenter 2.5 Update 6 or later system.
- Verify that you have Internet connectivity from the VirtualCenter 2.5 Update 6 or later or vCenter Server system. This allows new updates to be applied to the tool and allows you to view the reports and the Knowledge Base (KB) articles associated with the reports.

Procedure

1 On the VirtualCenter 2.5 Update 6 or later or vCenter Server system you are upgrading from, download the vCenter Server 5 installation package or insert the vCenter Server 5 installation DVD.

2 Take one of the following actions to start the Pre-Upgrade Checker.

- In the installation package or on the DVD, navigate to `\vpx\agentupgradecheck` and run the `AgentUpgradeChecker.exe` executable file.
- Start the vCenter Server installer `autorun.exe` and select **vCenter Host Agent Pre-Upgrade Checker** from the **Utility** list.

3 Select the DSN for the VirtualCenter or vCenter Server system you are upgrading from and select the login credentials that are appropriate for that DSN.

If you are not sure which credential type to select, check which authentication type is configured for the DSN (**Control Panel > Administrative Tools > ODBC Data Sources > System DSN**).

4 If the DSN requires a login for the credential type in use, enter a user name and password and click **Next**.

5 Select an option for scanning all hosts or specific hosts.

Option	Action
Scan all of the hosts	Select **Standard Mode** and click **Next**.
Specify hosts to scan	a Select **Custom Mode** and click **Next**. b Select the hosts to scan and click **Next**. To select all hosts in a cluster, double-click the cluster.

6 Click **Run Precheck**.

The tool takes 30-40 seconds for each host.

7 When the check is complete, click **Next**.

8 View the pre-upgrade reports.

- To view the report for an individual host, click the link next to the host name.
- To view a summary report for all hosts, click **View Report**.

You have a list of issues to resolve before you upgrade to vCenter Server 5.

What to do next

From the report, use the linked KB articles to research and resolve the issues for each host. After you resolve the issues, rerun the vCenter Host Agent Pre-Upgrade Checker. Repeat this process until you resolve all the reported issues, and proceed with your upgrade to vCenter Server 5.

Downtime During the vCenter Server Upgrade

When you upgrade vCenter Server, downtime is required for vCenter Server.

Expect downtime for vCenter Server as follows:

- The upgrade requires vCenter Server to be out of production for 40-50 minutes, depending on the size of the database. The database schema upgrade takes approximately 10-15 minutes of this time. This estimate does not include host reconnection after the upgrade.

  If Microsoft .NET Framework is not installed on the machine, a reboot is required before starting the vCenter Server installation.
- VMware Distributed Resource Scheduler does not work while the upgrade is in progress. VMware HA does work during the upgrade.

Downtime is not required for the ESX/ESXi hosts that vCenter Server is managing, or for virtual machines that are running on the hosts.

Download the vCenter Server Installer

You must download the installer for vCenter Server, the vSphere Client, and associated vCenter components and support tools.

Procedure

1 Download the zip file for vCenter Server from the VMware downloads page at http://www.vmware.com/support/.

2 Extract the files from the zip archive.

DNS Load Balancing Solutions and vCenter Server Datastore Naming

vCenter Server 5.x uses different internal identifiers for datastores than earlier versions of vCenter Server. This change affects the way that you add shared NFS datastores to hosts and can affect upgrades to vCenter Server 5.x.

vCenter Server versions before version 5.0 convert datastore host names to IP addresses. For example, if you mount an NFS datastore by the name \\nfs-datastore\folder, pre-5.0 vCenter Server versions convert the name nfs-datastore to an IP address like 10.23.121.25 before storing it. The original nfs-datastore name is lost.

This conversion of host names to IP addresses causes a problem when DNS load balancing solutions are used with vCenter Server. DNS load balancing solutions themselves replicate data and appear as a single logical datastore. The load balancing happens during the datastore host name-to-IP conversion by resolving the datastore host name to different IP addresses, depending on the load. This load balancing happens outside vCenter Server and is implemented by the DNS server. In vCenter Server versions before version 5.0, features

like vMotion do not work with such DNS load balancing solutions because the load balancing causes one logical datastore to appear as several datastores. vCenter Server fails to perform vMotion because it cannot recognize that what it sees as multiple datastores are actually a single logical datastore that is shared between two hosts.

To solve this problem, vCenter Server versions 5.0 and later do not convert datastore names to IP addresses when you add datastores. This enables vCenter Server to recognize a shared datastore, but only if you add the datastore to each host by the same datastore name. For example, vCenter Server does not recognize a datastore as shared between hosts in the following cases.

- The datastore is added by IP address to host1 and by *hostname* to host2.
- The datastore is added by *hostname* to host1, and by *hostname.vmware.com* to host2.

For vCenter Server to recognize a datastore as shared, you must add the datastore by exactly the same name to every host.

Datastore Names and Upgrades to vCenter Server 5.x

In vCenter Server versions before version 5.0, vCenter Server database stores datastore paths in the old format, as IP addresses. The upgrade to vCenter Server 5.x converts these paths to the new format. If you use a DNS load balancing solution with shared datastores, before you upgrade to vCenter Server 5.x, make sure that every shared datastore is mounted on each of its hosts with the exact same name.

The upgrade to vCenter Server 5.x might also fail from a lack of sufficient memory if you use a DNS load balancing solution with shared datastores. In a large vCenter Server database, the conversion of datastore paths to the new format can require a large amount of memory. See Knowledge Base article 2015055.

Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail

vCenter Server installation with a Microsoft SQL database fails when the database is set to compatibility mode with an unsupported version.

Problem

The following error message appears: `The DB User entered does not have the required permissions needed to install and configure vCenter Server with the selected DB. Please correct the following error(s): %s`

Cause

The database version must be supported for vCenter Server. For SQL, even if the database is a supported version, if it is set to run in compatibility mode with an unsupported version, this error occurs. For example, if SQL 2008 is set to run in SQL 2000 compatibility mode, this error occurs.

Solution

- Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version. See "vCenter Server Database Patch and Configuration Requirements," on page 33

vCenter Server Upgrade Fails When You Restore a Microsoft SQL 2000 Backup to the vCenter Server Database

A vCenter Server upgrade fails if you restore a Microsoft SQL 2000 database backup to the vCenter Server database.

Problem

When the failure occurs, the following error message appears: `DBuser entered doesn't have the required permissions to install and configure vCenter Server with the selected DB`.

Cause

This problem can occur when you upgrade to vCenter Server from VirtualCenter 2.x. VirtualCenter 2.x supports SQL 2000, which VMware does not support for vCenter Server 5.0. When you restore a backup from SQL Server 2000 on SQL Server 2005, the restored database is set to compatibility level 80, which is compatible with SQL Server 2000. The minimum supported compatibility level for vCenter Server 5.0 databases is 90, which is compatible with SQL Server 2005.

Solution

- Before you upgrade to vCenter Server, change the compatibility level to 90, for compatibility with SQL Server 2005, or to 100, for compatibility with SQL Server 2008.

```
ALTER DATABASE AdventureWorks SET SINGLE_USER;
GO
EXEC sp_dbcmptlevel AdventureWorks, 90;
GO
ALTER DATABASE AdventureWorks SET MULTI_USER;
GO
```

Updating Version 3.5 Hosts in High Availability Clusters Before Upgrading vCenter Server

Before you upgrade vCenter Server to version 5.0, make sure that any ESX 3.5 hosts that are in a vSphere HA cluster are updated to a patch level that supports High Availability.

If a version 3.5 ESX or ESXi host is in a vSphere HA cluster and is not updated to a patch level that supports High Availability, you cannot add that host to the HA cluster or remove it from maintenance mode after the associated vCenter Server is upgraded to version 5.0.

Update ESX 3.5 hosts to ESX350-201012401-SG PATCH, and update ESXi 3.5 hosts to ESXe350-201012401-I-BG PATCH. If you have updated your version 3.5 hosts to these patch levels but you still cannot add the hosts to a HA cluster or remove them from maintenance mode after the associated vCenter Server is upgraded to version 5.0, you might need to apply the following patches.

Apply these patches to ESX 3.5 hosts:

- ESX350-201012401-SG PATCH
- ESX350-201012402-BG PATCH
- ESX350-201012404-BG PATCH
- ESX350-201012405-BG PATCH
- ESX350-201012406-BG PATCH
- ESX350-201012407-BG PATCH
- ESX350-201012408-SG PATCH

- ESX350-201012409-SG PATCH
- ESX350-201012410-BG PATCH

Apply these patches to ESXi 3.5 hosts:

- ESXe350-201012401-I-BG PATCH
- ESXe350-201012402-T-BG PATCH

For information about updating version 3.5 hosts with patches, see the *ESX Server 3 Patch Management Guide*. You can download patches from the VI3 Patches and Updates page at http://www.vmware.com/patch/download/.

Upgrade to vCenter Server 5.0

Upgrade vCenter Server 4.x to vCenter Server 5.0 on the same machine if the vCenter Server 4.x instance is on a 64-bit machine.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

In-place upgrade to vCenter 5.0 is not supported on Microsoft Windows XP.

NOTE If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

If the vCenter Server that you are upgrading from has plug-ins or plug-in versions that are incompatible with vCenter Server 5.0, for example vSphere Converter or Update Manager, these plug-ins will be unregistered during the upgrade process.

Prerequisites

- See "Prerequisites for the vCenter Server Upgrade," on page 30 for requirements for the vCenter Server system and for the database.
- Download the vCenter Server 5.0 installer from the VMware Web site.
- Back up the existing vCenter Server database.
- Close all instances of the VI Client and the vSphere Client.
- Make sure that you have a valid license key.
- You must be logged in as Administrator on the Windows machine you are installing vCenter Server on.
- If VMware Guided Consolidation Services is installed on the existing vCenter Server, uninstall it.

Procedure

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

2 Select **vCenter Server**™ and click **Install.**

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.

IMPORTANT If you do not enter a license key, your license will expire. After the installation, you can connect to the vCenter Server with the vSphere Client and reenter the license key.

4 Select the DSN.

This page appears if the installer is unable to determine the DSN for the database to be upgraded. The DSN must be a 64-bit DSN. Depending on the database type, the DSN might be selected, or there might be only one option.

5 Type the database user name and password for the DSN.

If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.

6 Select whether to upgrade the vCenter Server database.

- Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
- Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

  You cannot continue the upgrade.

7 Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

8 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

9 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use SYSTEM account** checkbox, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the SYSTEM account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use SYSTEM account** checkbox, type the account password and the fully qualified domain name of the vCenter Server host and click **Next**.

10 Select a folder to install vCenter Inventory Service.

NOTE The folder size might grow large.

11 Enter port numbers to connect to vCenter Server.

12 Type the port numbers for Inventory Service or accept the port numbers shown in the Configure Ports for Inventory Service window.

13 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 "vCenter Server and vSphere Client Hardware Requirements," on page 17.

14 (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.

What to do next

Upgrade the vSphere Client to version 5.0. This step prevents compatibility problems that might interfere with the proper operation of the vSphere Client. See "Upgrade the vSphere Client," on page 61. Review the topics in "After You Upgrade vCenter Server," on page 60 for other postupgrade actions you might want to take.

Upgrade to vCenter Server on a Different Machine and Upgrade the Database

When you upgrade to vCenter Server, you can migrate vCenter Server to a new machine. One reason for doing this is to move from a 32-bit machine to a 64-bit machine.

You can also use the data migration tool to migrate a SQL Server Express database that is installed by the vCenter Server installer on the same machine as vCenter Server. If you use a different database that is installed on the vCenter Server machine, you must back up and move the database manually to the new machine. If the database is installed on a different machine from vCenter Server, you can leave the database in place and create a DSN on the destination machine to connect to it.

The VirtualCenter or vCenter Server configuration settings that you can migrate with the tool include:

- LDAP data.
- Port settings for the HTTP, HTTPS, heartbeat, Web services, LDAP, and LDAP SSL ports.
- Certificates stored in the SSL folder.
- License.
- Database data for a bundled SQL Server Express database only.

If VMware vCenter Update Manager or vCenter Orchestrator is installed on the same machine as vCenter Server, you can use the data migration tool to migrate configuration data for these products. You can also use the tool to migrate the vCenter Update Manager database if it is a SQL Server Express database installed on the same machine as vCenter Update Manager and vCenter Server. You cannot use the data migration tool to migrate the vCenter Orchestrator database. See the documentation for vCenter Update Manager and vCenter Orchestrator for information about upgrading these products.

IMPORTANT If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Prerequisites

If you are using a remote database, either remove any ESX Server 2.x hosts from the VirtualCenter or vCenter Server inventory or upgrade these hosts. If you are not using a remote database, you do not need to remove ESX Server 2.x hosts from the VirtualCenter or vCenter Server inventory or upgrade them. However, they will not be connected to the vCenter Server after the upgrade.

Stop the VMware VirtualCenter Server service before you perform this upgrade.

Procedure

1 Back Up and Move a Local vCenter Server Database on page 44

Before you upgrade vCenter Server, back up the vCenter Server database. Migrating vCenter Server with a local database to a new machine, you have several options for moving the database to the new machine.

2 Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool on page 50

The data migration tool allows you to back up VirtualCenter or vCenter Server configuration data such as port settings, SSL certificates, and licensing information. The data migration tool can restore these settings when you upgrade to vCenter Server on a new 64-bit host machine.

3 Create a 64-Bit DSN on page 51

The vCenter Server system must have a 64-bit DSN. This requirement applies to all supported databases.

4 Restore the vCenter Server Configuration and Install vCenter Server on the Destination Machine on page 51

Use the data migration tool to start the vCenter Server installer and restore the vCenter Server configuration to the destination machine.

5 Update the vCenter Server Name for Plug-Ins on page 56

When you migrate the vCenter Server configuration to a destination machine that does not have the same name as the source machine, you must update the plug-ins to use the new machine name. Plug-ins registered to the vCenter Server system cannot access the destination vCenter Server machine until this update is complete.

6 Migrate a License Server Installed on the Same Machine as vCenter Server on page 57

If the license server was installed with vCenter Server on the source machine, the data migration tool cannot migrate the license server to the destination machine. You must migrate the license configuration manually.

Back Up and Move a Local vCenter Server Database

Before you upgrade vCenter Server, back up the vCenter Server database. Migrating vCenter Server with a local database to a new machine, you have several options for moving the database to the new machine.

If your database is remote from VirtualCenter or vCenter Server, you do not need to move the database after you back it up.

Procedure

- If your database is local to VirtualCenter or vCenter Server, and you want it to remain local after the upgrade, choose one the following options.

Option	Description
Microsoft SQL Server Express database	If the database was installed by the vCenter Server installer, back up the database, and move the database along with other configuration data using the data migration tool. If the SQL Server Express database was not installed by the vCenter Server installer, back up the database and restore it onto the machine that you are installing vCenter Server on.
Microsoft SQL Server database	Do one of the following, but consider the downtime required. Consult your organization's database administrator. ■ Back up the database, detach the database, and attach it to the machine that you are installing vCenter Server on. ■ Back up the database, and restore it onto the machine that you are installing vCenter Server on.
Other local databases	Back up the database, and restore it onto the machine that you are installing vCenter Server on.

What to do next

Back up the VirtualCenter or vCenter Server configuration using the data migration tool.

Back Up and Restore a Microsoft SQL Database

Before you perform an upgrade to vCenter Server on a new machine, you might want to move the database. For example, if your database currently resides on the same machine as vCenter Server, you might want to move it to the same machine you move vCenter Server to. To move a Microsoft SQL Server database, you can perform a backup and restore operation.

Consult your database administrator or see your database documentation about backing up and restoring databases.

The machine with the VirtualCenter 2.5 Update 6 or vCenter Server 4.x database is called the source machine. The machine that the vCenter Server 5.0 database will reside on is called the destination machine.

Prerequisites

- Verify that you have a VirtualCenter 2.5 Update 6 or vCenter Server 4.x system running with a local or remote Microsoft SQL Server database.
- Verify that Microsoft SQL Server and Microsoft SQL Server Management Studio are installed on the source machine and the destination machine.

Procedure

1. On the source machine, stop the VirtualCenter service.
   a. Select **Start > Control Panel > Administrative Tools > Services**.
   b. Right-click **VMware VirtualCenter Server** and select **Stop**.

      The Status changes from Started to blank.
2. In SQL Server Management Studio, make a full back up of the source machine database.
3. Copy the backup file (`.bak`) to the `C:\` drive on the destination machine.
4. On the destination machine, open SQL Server Management Studio and right-click the **Databases** folder.
5. Select **New Database**, enter the source machine database name, and click **OK**.

6 Right-click the new database icon and select **Task > Restore > Database**.

7 Select **From Device** and click **Browse**.

8 Click **Add**, navigate to the backup file, and click **OK**.

9 In the Restore Database window, select the `.bak` file check box.

10 On the Options page, select the **Overwrite the existing database** check box and click **OK**.

The original database is restored onto the new database, which you can use for the upgrade to vCenter Server 5.0.

What to do next

See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50.

Detach and Attach a Microsoft SQL Server Database

Before you perform an upgrade to vCenter Server on a 64-bit machine, you can optionally detach the VirtualCenter or vCenter Server database on the source machine, copy the files to the destination machine, and attach the database on the destination machine. This detach-and-attach action is an alternative to the backup and restore operation.

Consult your database administrator or see your database documentation about detaching and attaching databases.

The machine with the VirtualCenter 2.5 Update 6 or vCenter Server 4.x database is called the source machine. The machine on which the vCenter Server 5.0 database will reside is called the destination machine.

Prerequisites

- Make a full backup of the database.
- Verify that you have a VirtualCenter 2.5 Update 6 or vCenter Server 4.x system running with a local or remote Microsoft SQL Server database.
- Verify that Microsoft SQL Server and Microsoft SQL Server Management Studio are installed on the source machine and the destination machine.

Procedure

1 On the source machine, stop the VirtualCenter service.

   a Select **Start > Control Panel > Administrative Tools > Services**.

   b Right-click **VMware VirtualCenter Server** and select **Stop**.

   The Status changes from Started to blank.

2 In the SQL Server Management Studio, open the **Databases** directory.

3 Right-click the source database and select **Tasks > Detach**.

4 Select the database and click **OK**.

5 When the detach operation is complete, copy the data files (`.mdf` and `.ldf`) to the destination machine's database folder.

   By default, the database folder is `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data`.

6 In SQL Server Management Studio on the destination machine, right-click the **Databases** directory and select **Attach**.

7 Select the `.mdf` file that you copied to the destination machine's database folder and click **OK**.

The database from the source machine is attached to the destination machine.

What to do next

See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50.

Back Up and Restore an Oracle Database

Before you perform an upgrade to vCenter Server on a different machine, you might want to move the database to the new vCenter Server machine. To move the database, back up the database on the existing machine and restore the database on the new machine. Moving the database is optional.

Consult your database administrator or see your database documentation about backing up and restoring databases.

The machine with the VirtualCenter 2.5 Update 6 or vCenter Server 4.0 database is called the source machine. The machine on which the vCenter Server 5.0 database will reside is called the destination machine.

Prerequisites

Verify that you have a VirtualCenter 2.5 Update 6 or vCenter Server 4.0 system running with a local or remote Oracle 10g or Oracle 11g database.

Procedure

1 On the source machine, stop the VirtualCenter service.

   a Select **Start > Control Panel > Administrative Tools > Services**.

   b Right-click **VMware VirtualCenter Server** and select **Stop**.

   The Status changes from Started to blank.

2 On the source machine, log in to Oracle SQL*Plus as the VirtualCenter 2.5 or vCenter Server 4.0 database user.

3 Export the database as a `.dmp` file.

4 Copy the `.dmp` file onto the `C:\` drive of the destination machine.

5 In Oracle SQL*Plus, run the following command to create the tablespace.

```
create tablespace vctest datafile 'c:\vctest.dbf' size 100m autoextend on;
```

6 Run the following command to create a user.

```
create user VCUSER identified by CENSORED default tablespace vctest;
```

7 Import the `.dmp` file into the Oracle 64-bit database on the destination machine.

8 Verify that all the table data is imported.

The original database is restored onto the new machine, which you can use for the upgrade to vCenter Server 5.0.

What to do next

See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50.

Back Up and Restore an IBM DB2 Database

Before you perform an upgrade to vCenter Server on a different machine, you might want to move the database to the new vCenter Server machine. To move the database, back up the database on the existing machine and restore the database on the new machine. Moving the database is optional.

Moving the database is optional. Consult your database administrator or see your database documentation for information about backing up and restoring databases. The machine with the vCenter Server 4.0 Update 1 or vCenter Server 4.1 database is called the source machine. The machine on which vCenter Server 5.0 database resides is called the destination machine.

Prerequisites

- Your machine has a vCenter 4.0 Update 1 or vCenter Server 4.1 system installed and running with a local or remote IBM DB2 database version that is supported for vCenter Server 5.0. See "vCenter Server Database Patch and Configuration Requirements," on page 33.
- You are a system administrator to perform backup or restore operations.
- You are using archival logging to create backup image of tablespaces. If you are using circular logging, you cannot create tablespace backup image.
- You have installed DB2 database Control Center on the source machine and the destination machine.

Procedure

1 On the source machine, stop the VirtualCenter service.

   a Select **Start > Control Panel > Administrative Tools > Services**.

   b Right-click **VMware VirtualCenter Server** and select **Stop**.

   The Status changes from Started to blank.

2 (Optional) If the DB2 database is in use, stop and start the database.

3 On the source machine, use Backup Database wizard from the Control Center to back up the DB2 database attached to the source machine.

   a Right-click the database to be backed up, select **Backup**, and follow the Backup wizard.

   b Select the **File System** media type and specify the backup image location on the source machine.

   c Select **Full Backup Type** to back up all data.

4 Copy the backup image file to the destination machine.

   NOTE On all operating systems, use the following format for file names of backup images: DB_alias.Type.Inst_name.NODEnnnn.CATNnnnn.timestamp.Seq_num.

5 Copy the backup image file to the destination machine.

6 On the destination machine, open the Control Center.

7 Right-click the **All Databases** folder and select **Create Databases > From Backup**.

8 Specify the name of the database that is being restored, and enter a new database name.

9 Enter the following backup image information.

   a Enter the file system media type.

   b Click **Add** and browse to the file location on the destination machine.

   c Click **Add** and browse to the backup image.

   d Enter the date and time of the backup image file.

10 Click **Finish**.

   The original database is restored.

What to do next

See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50.

Variables for IBM DB2 Backup and Restore Commands

The commands to back up and restore an IBM DB2 database use these variables.

Table 4-4. `backup` Command Variables

Variable	Description
DatabaseName	The name assigned to the database.
UserName	The user name of the administrator.
Password	Password of the administrator.
TS_Name	The name of the specific tablespaces to be backed up.
Location	The directory to store the backup image. If you do not specify a location, the file is stored in the current directory.
NumBuffers	The number of buffers required for the backup operation. If you do not specify the number, by default the system uses two buffers.
BufferSize	The size, in pages, that each buffer uses to perform the backup operation. The size of each buffer used by this operation is based on the value of the `backbufsz` DB2 Database Manager configuration parameter.
ParallelNum	The number of tablespaces that the system can read in parallel during a backup operation.
INCREMENTAL	The backup operation creates an incremental backup image, which is a copy of all data that were updated since the last successful backup.

Table 4-5. `restore` Command Variables

Variable	Description
DatabaseName	The name assigned to the database.
UserName	The user name of the administrator.
Password	Password of the administrator.
TS_Name	The name of the specific tablespaces to be backed up.
SourceLocation	The directory where the backup image is stored.
Timestamp	Timestamp of a particular backup image, which is used for search during restore. If you do not specify a timestamp, only one backup image is available at the source location.
TargetLocation	The directory to store the restored database, if you are using the backup image to create a new database.
TargetAlias	The alias for the new database.
LogsLocation	The directory where log files for the new database are stored.
NumBuffers	The number of buffers used for the restore operation. If you do not specify the number, by default the system uses two buffers.
BufferSize	The size, in pages, that each buffer uses to perform the restore operation. The size of each buffer used by this operation is based on the value of the `backbufsz` DB2 Database Manager configuration parameter.
ParallelNum	The number of tablespaces that the system can read in parallel during a restore operation.

Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool

The data migration tool allows you to back up VirtualCenter or vCenter Server configuration data such as port settings, SSL certificates, and licensing information. The data migration tool can restore these settings when you upgrade to vCenter Server on a new 64-bit host machine.

If your database is a SQL Server Express database that is local to the VirtualCenter or vCenter Server machine, the data migration tool will back up the database and restore it to the destination machine.

If VMware vCenter Orchestrator is installed on the same machine as VirtualCenter or vCenter Server, the data migration tool will back up the vCenter Orchestrator configuration and restore it to the destination machine. The data migration tool does not back up and restore the vCenter Orchestrator database. See *Installing and Configuring VMware vCenter Orchestrator* for information about upgrading vCenter Orchestrator using the data migration tool.

If VMware vCenter Update Manager is installed on the same machine as VirtualCenter or vCenter Server, the data migration tool will back up the vCenter Update Manager configuration and restore it to the destination machine. If vCenter Update Manager uses a SQL Server Express database that is local to the source machine, the data migration tool will back up the database and restore it to the destination machine. The data migration tool does not back up and restore patch binaries. See *Installing and Administering VMware vSphere Update Manager* for information about upgrading vCenter Update Manager with the data migration tool.

Prerequisites

- Verify that a supported version of VirtualCenter or vCenter Server is installed on the source machine:
  - VirtualCenter 2.5 Update 6 or later.
  - vCenter Server 4.0.x and its update releases.

  NOTE vCenter Server 4.1.x is not supported for the data migration tool. vCenter Server 4.1.x requires a 64-bit host machine. Because vCenter Server 4.1.x cannot be installed on 32-bit host machines, there is no case for migration from a 32-bit machine to a 64-bit machine.
- Stop the VMware VirtualCenter Server service before you back up the configuration.
- If the `\datamigration\data\` folder exists from a previous backup attempt, backup cannot proceed. Remove or rename this folder before you back up the vCenter Server configuration.
- If you are using a bundled database for VirtualCenter 2.5 Update 6 or later or vCenter Server 4.x, make sure that named pipes are not disabled and that the pipe name is correct. Change the default pipe name to `\\.\pipe\sql\query`.
- If you are using a bundled database, do not change the DSN name. Use "VMware VirtualCenter' for the DSN name. If you change the DSN name, the backup operation will fail.

Procedure

1. As Administrator on the Windows system, insert the VMware vCenter Server Installation DVD or double-click `autorun.exe`.
2. Click **Explore media**.
3. Open the `datamigration` folder and extract the `datamigration.zip` archive to a writeable local file system on the source VirtualCenter or vCenter Server machine.
4. From the Windows command prompt, change to the `datamigration` folder and type **`backup.bat`** to run the backup script of the data migration tool.

5 Respond to the script prompts.

The script checks the vCenter Server version, database type, vCenter Update Manager configuration (if installed), and vCenter Orchestrator configuration (if installed) to determine whether they are compatible with the data migration tool.

6 If VMware vCenter Update Manager is not installed, enter **y** when prompted to continue the backup.

The VirtualCenter or vCenter Server configuration data and the SQL Server Express database (if applicable) are copied to the `\data` folder in the extracted folder. The VirtualCenter or vCenter Server database instance is upgraded to be compatible with vCenter Server 5.0.

7 Check `\logs\backup.log` in the `datamigration` folder for errors.

- If you find no errors, the data backup was successful.
- If you find errors, correct the source of the error and rerun `backup.bat`.

What to do next

- If your database is the bundled SQL Server Express database local to the vCenter Server machine, see "Restore the vCenter Server Configuration and the Bundled Database and Install vCenter Server on the Destination Machine," on page 52.
- If you are using another database, see "Create a 64-Bit DSN," on page 51 and "Restore the vCenter Server Configuration and Nonbundled Database and Install vCenter Server on the New Machine," on page 54.

Create a 64-Bit DSN

The vCenter Server system must have a 64-bit DSN. This requirement applies to all supported databases.

If you use the data migration tool to migrate a SQL Server Express database located on the vCenter Server system to a new system, you do not need to create the 64-bit DSN. The data migration tool creates the DSN as part of the installation process. For other databases that are not bundled with vCenter Server, you must create a 64-bit DSN.

Procedure

1 Select **Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Use the application to create a system DSN.

If you have a Microsoft SQL database, create the system DSN for the SQL Native Client driver.

3 Test the connectivity.

The system now has a DSN that is compatible with vCenter Server. When the vCenter Server installer prompts you for a DSN, select the 64-bit DSN.

Restore the vCenter Server Configuration and Install vCenter Server on the Destination Machine

Use the data migration tool to start the vCenter Server installer and restore the vCenter Server configuration to the destination machine.

- Restore the vCenter Server Configuration and the Bundled Database and Install vCenter Server on the Destination Machine on page 52

  After you use the data migration tool to back up the configuration of a vCenter Server system with the bundled SQL Server Express database, you complete the migration to a new machine by using the data migration tool to install vCenter Server and restore the vCenter Server configuration on the destination machine.

- Restore the vCenter Server Configuration and Nonbundled Database and Install vCenter Server on the New Machine on page 54

  After you use the data migration tool to back up the configuration of a vCenter Server system with a nonbundled database, you complete the migration to a new machine by using the data migration tool to install vCenter Server and restore the vCenter Server configuration on the destination machine.

Restore the vCenter Server Configuration and the Bundled Database and Install vCenter Server on the Destination Machine

After you use the data migration tool to back up the configuration of a vCenter Server system with the bundled SQL Server Express database, you complete the migration to a new machine by using the data migration tool to install vCenter Server and restore the vCenter Server configuration on the destination machine.

Use this procedure if you are migrating a vCenter Server that uses the bundled SQL Server Express database. The data migration tool restores the database to the new machine and launches the vCenter Server installer.

If you are migrating a vCenter Server that uses a database other than the bundled SQL Server Express database, see "Restore the vCenter Server Configuration and Nonbundled Database and Install vCenter Server on the New Machine," on page 54.

VMware recommends that you use the same host name for the destination machine that you used for the source machine.

Prerequisites

- Use the data migration tool to back up the VirtualCenter or vCenter Server configuration on machine you are migrating from. See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50
- Ensure that the destination vCenter Server machine has access to all other systems that it must connect to, such as the domain server, Windows Active Directory server with vCenter user accounts, database server, and license server.
- Ensure that Microsoft Windows Installer (MSI) 4.5 is installed on the destination machine.
- Ensure that Microsoft .NET Framework 3.5 is installed on the destination machine.
- Ensure that the VIM_SQLEXP or SQLEXP_VIM databases do not exist on the destination machine. These databases might be left after you uninstall vCenter Server 4.0, 4.1, or 5.0. Installing vCenter Server on a machine that has either of those databases is not supported. Before running the data migration scripts, uninstall VIM_SQLEXP or SQLEXP_VIM databases, and any file system directories pertaining to previous vCenter Server installations. For best results, use a machine on which vCenter Server has never been installed.
- After installing all prerequisite software, reboot the server.

Procedure

1. Copy the `datamigration` folder from the source machine to the destination machine.
2. Insert the vCenter Server installation media into the DVD-ROM drive on the destination machine, or copy the installation ISO image to the destination machine.
3. From the Windows command prompt, change to the `datamigration` folder copied from the source machine and type **`install.bat`**.
4. If the name of the destination machine is different from the name of the source machine, type **`y`** to continue.

5 Type the path to the vCenter Server installation media.

For example, if the installation media is in `D:\Temp\VMware-VIMSetup-en-5.0-build number`, enter **`D:\Temp\VMware-VIMSetup-en-5.0-build number`**.

The install script verifies that migration data is present, and opens the vCenter Server installer.

6 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.

IMPORTANT If you do not enter a license key, your license will expire. After the installation, you can connect to the vCenter Server with the vSphere Client and reenter the license key.

7 Select **Install a Microsoft SQL Server 2008 Express instance (for small-scale deployments)**.

8 Type the password for the vCenter Service user account, if the user account is specified.

By default, **Use SYSTEM Account** is selected.

9 Type the fully qualified domain name (FQDN).

10 Either accept the default destination folders for vCenter Server and Inventory Service or click **Change** to select another location.

The installation path cannot have commas (`,`) or periods (`.`).

NOTE To install the vCenter Server on a drive other than `C:`, verify that the `C:\WINDOWS\Installer` directory has enough space to install the Microsoft Windows Installer `.msi` file. If you do not have enough space, your vCenter Server installation might fail.

11 Type the port numbers for vCenter Server or accept the default port numbers in the Configure Ports window.

The port numbers displayed are those that were backed up from the source VirtualCenter or vCenter Server installation.

12 Type the port numbers for Inventory Service or accept the port numbers shown in the Configure Ports for Inventory Service window.

13 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*.

14 (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.

15 Click **Install**, and when the vCenter Server installation finishes, click **Finish**.

The data migration tool restores the backed up configuration data. The installer wizard opens and installs the vCenter Inventory Service and VMware vSphere Profile-Driven Storage.

16 After the vCenter Inventory Service and vSphere Profile-Driven Storage are installed, click **Finish** in the Installation Completed window.

17 If you used the data migration tool to back up VMware vCenter Update Manager configuration data, complete the steps in the Update Manager installation wizard to install vCenter Update Manager and restore the configuration. See *Installing and Administering VMware vSphere Update Manager*.

vCenter Server is installed, and the settings that you backed up are restored. The SQL Server Express database is also restored on the new machine. After the installation is complete, vCenter Server is started.

What to do next

- If the new vCenter Server machine has a different name than the source machine, update plug-ins and other solutions that access the vCenter Server system with the name of the new machine. See "Update the vCenter Server Name for Plug-Ins," on page 56.
- If a license server was installed on the source machine, install the license server on the destination machine and migrate the licenses. See "Migrate a License Server Installed on the Same Machine as vCenter Server," on page 57.
- See "After You Upgrade vCenter Server," on page 60.

Restore the vCenter Server Configuration and Nonbundled Database and Install vCenter Server on the New Machine

After you use the data migration tool to back up the configuration of a vCenter Server system with a nonbundled database, you complete the migration to a new machine by using the data migration tool to install vCenter Server and restore the vCenter Server configuration on the destination machine.

Perform this procedure if you are migrating a vCenter Server that uses a database other than the bundled SQL Server Express database. The data migration tool restores the database to the new machine and launches the vCenter Server installer.

If you are migrating a vCenter Server that uses the bundled SQL Server Express database, see "Restore the vCenter Server Configuration and the Bundled Database and Install vCenter Server on the Destination Machine," on page 52.

Prerequisites

- Use the data migration tool to back up the VirtualCenter or vCenter Server configuration on machine you are migrating from. See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50
- Ensure that the destination vCenter Server machine has access to all other systems that it must connect to, such as the domain server, Windows Active Directory server with vCenter user accounts, database server, and license server.
- Ensure that Microsoft .NET Framework 3.5 is installed on the destination machine.
- Ensure that the VIM_SQLEXP or SQLEXP_VIM databases do not exist on the destination machine. These databases might be left after you uninstall vCenter Server 4.0, 4.1, or 5.0. Installing vCenter Server on a machine that has either of those databases is not supported. Before running the data migration scripts, uninstall VIM_SQLEXP or SQLEXP_VIM databases, and any file system directories pertaining to previous vCenter Server installations. For best results, use a machine on which vCenter Server has never been installed.
- Restart the database before you start the database restore process.

Procedure

1. Copy the `datamigration` folder from the source machine to the destination machine.
2. Insert the vCenter Server installation media into the DVD-ROM drive on the destination machine, or copy the installation ISO image to the destination machine.
3. From the Windows command prompt, change to the `datamigration` folder copied from the source machine and type **`install.bat`**.
4. If the name of the destination machine is different from the name of the source machine, type **`y`** to continue.

5 Type the path to the vCenter Server installation media.

For example, if the installation media is in `D:\Temp\VMware-VIMSetup-en-5.0-build number`, enter **`D:\Temp\VMware-VIMSetup-en-5.0-build number`**.

The install script verifies that migration data is present, and opens the vCenter Server installer.

6 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.

IMPORTANT If you do not enter a license key, your license will expire. After the installation, you can connect to the vCenter Server with the vSphere Client and reenter the license key.

7 If you are using a remote database, enter the information for the remote database.

a Click **Use an existing supported database**.

b Select the 64-bit DSN that was used for the database on the 32-bit source machine.

c Enter the user name and password for the DSN.

If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.

d Select **Upgrade existing vCenter Server database** and select the **I have taken a backup of the existing vCenter Server database and SSL certificates** check box.

8 Select how to upgrade vCenter Agent.

Option	Description
Automatic	vCenter Agent is upgraded on all hosts in the vCenter Server inventory.
Manual	All hosts are disconnected from vCenter Server. To upgrade vCenter Agent, reconnect the host to vCenter Server. Select Manual if one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ The number of hosts in the vCenter Server inventory is large, and you anticipate that upgrading vCenter Agent on all hosts would negatively affect vCenter Server performance.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

9 Type the password for the vCenter Service user account, if the user account is specified.

By default, **Use SYSTEM Account** is selected.

10 Type the fully qualified domain name (FQDN).

11 Either accept the default destination folders for vCenter Server and Inventory Service or click **Change** to select another location.

The installation path cannot have commas (`,`) or periods (`.`).

NOTE To install the vCenter Server on a drive other than `C:`, verify that the `C:\WINDOWS\Installer` directory has enough space to install the Microsoft Windows Installer `.msi` file. If you do not have enough space, your vCenter Server installation might fail.

12 Type the port numbers for vCenter Server or accept the default port numbers in the Configure Ports window.

The port numbers displayed are those that were backed up from the source VirtualCenter or vCenter Server installation.

13 Type the port numbers for Inventory Service or accept the port numbers shown in the Configure Ports for Inventory Service window.

14 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*.

15 (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.

16 Click **Install**, and when the vCenter Server installation finishes, click **Finish**.

The data migration tool restores the backed up configuration data. The installer wizard opens and installs the vCenter Inventory Service and VMware vSphere Profile-Driven Storage.

17 After the vCenter Inventory Service and vSphere Profile-Driven Storage are installed, click **Finish** in the Installation Completed window.

18 If you used the data migration tool to back up VMware vCenter Update Manager configuration data, complete the steps in the Update Manager installation wizard to install vCenter Update Manager and restore the configuration. See *Installing and Administering VMware vSphere Update Manager*.

19 Check the `\logs\restore.log` file in the `datamigration` folder, and verify that no errors occurred during the restore process.

vCenter Server is installed, and the settings that you backed up are restored. The remote database is upgraded. After the installation is complete, vCenter Server is started.

What to do next

- If the new vCenter Server machine has a different name than the source machine, update plug-ins and other solutions that access the vCenter Server system with the name of the new machine. See "Update the vCenter Server Name for Plug-Ins," on page 56.
- If a license server was installed on the source machine, install the license server on the destination machine and migrate the licenses. See "Migrate a License Server Installed on the Same Machine as vCenter Server," on page 57.
- See "After You Upgrade vCenter Server," on page 60.

Update the vCenter Server Name for Plug-Ins

When you migrate the vCenter Server configuration to a destination machine that does not have the same name as the source machine, you must update the plug-ins to use the new machine name. Plug-ins registered to the vCenter Server system cannot access the destination vCenter Server machine until this update is complete.

Procedure

1 Open the `extension.xml` file for the plug-in in a text editor.

The `extension.xml` file is located in the folder for the plug-in in `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions\`. For example, the `extension.xml` file for the vCenter Storage Monitoring plug-in is `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions\com.vmware.vim.sms\extension.xml`.

2 Edit the contents of the `<url>` tag to replace the name of the source vCenter Server system with the name of the new vCenter Server system.

   For example: If the new server name is vcenter.example.com, the `<url>` tag might read `<url>http://vcenter.example.com:80/sms/smService-web/health.xml</url>`.

3 Save the `extension.xml` file.

4 Re-register the extension with vCenter Server.

Migrate a License Server Installed on the Same Machine as vCenter Server

If the license server was installed with vCenter Server on the source machine, the data migration tool cannot migrate the license server to the destination machine. You must migrate the license configuration manually.

Prerequisites

If you do not have the license server installer, download it from the VMware Web site.

Procedure

1 Install the license server on the destination machine.

2 Copy the license files from the license folder on the source machine to the license folder on the destination machine.

   By default, the license folder is `C:\Program Files\VMware\VMware License Server\Licenses\`.

3 Reload the licenses.

   a Select **Start > Programs > VMware > VMware License Server > VMware License Server Tools**.

   b Click the **Start/Stop/Reread** tab.

   c Select the VMware License Server.

   d Click **ReRead License File**.

4 Update vCenter Server licensing settings with the license server machine name.

   a Connect to the vCenter Server using the vSphere Client.

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

   c Select **Licensing**.

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

   For example: 27000@licenseservername.companyname.com

   e Click **OK**.

The license server and license configuration are migrated to the destination machine.

Upgrade the VMware vCenter Server Appliance

For major upgrades to the vCenter Server Appliance, you can deploy a new version of the appliance and import the network identity of your existing vCenter Server Appliance.

For minor updates to the vCenter Server Appliance, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 58, "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 59, and "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 60.

NOTE Version 5.0.1 of the vCenter Server Appliance uses PostgreSQL for the embedded database instead of IBM DB2, which was used in vCenter Server Appliance 5.0. If you use the embedded database with the vCenter Server Appliance, when you upgrade from version 5.0 to version 5.0.1, the embedded IBM DB2 database is migrated to a PostgreSQL database. The configuration state of your existing database is preserved and the schema is upgraded to be compatible with vCenter Server Appliance 5.0.1.

Procedure

1 Deploy the new version of the vCenter Server Appliance.

  The new appliance has a default network configuration, and the vCenter Server service is unconfigured and disabled.

2 Connect to both the old and new appliances in separate browser windows.

3 In the **Upgrade** tab of the new appliance, select **destination** for the appliance role, and click **Set role**.

4 In the **Upgrade** tab of the old appliance, select **source** for the appliance role, and click **Set role**.

5 In each appliance, click **Establish Trust**.

  The local appliance key appears.

6 In the new appliance, copy the local appliance key.

7 Paste the local appliance key into the **Remote appliance key** field of the old appliance.

8 Click **Import remote key** in the old appliance.

9 In the old appliance, copy the local appliance key.

10 Paste the local appliance key into the **Remote appliance key** field of the new appliance.

11 Click **Import remote key** in the new appliance.

12 In the new appliance, click **Import**, and click **Start import**.

  The new appliance shuts down the old appliance and assumes the network identity of the old appliance. This process can take several minutes. When the import is complete, the new vCenter Server Appliance starts.

Update the VMware vCenter Server Appliance from a VMware.com Repository

You can set the vCenter Server Appliance to update itself from a public repository on the VMware.com Web site.

To update the vCenter Server Appliance from a zipped update bundle that you download to your own internal repository, see "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 59. To update the vCenter Server Appliance from the virtual CD-ROM drive of the appliance, see "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 60. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 58.

Procedure

1 Open the management vCenter Virtual Appliance web interface on port 5480.

2 In the Update tab, click **Settings**.

3 (Optional) Under Automatic Updates, set and schedule the vCenter Server Appliance to check for and install updates.

4 Under Update Repository, select **Use Default Repository**.

The default repository is set to the correct VMware.com URL.

5 Click **Save Settings**.

6 Click **Status**.

7 Under Actions, click **Check Updates** or **Install Updates**.

Update the VMware vCenter Server Appliance from a Zipped Update Bundle

If your Internet access is restricted, you can set up your own internal repository for updates, instead of updating from a VMware public repository. You can download updates as a zipped update bundle.

To update the vCenter Server Appliance from a VMware public repository, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 58. To update the vCenter Server Appliance from the virtual CD-ROM drive of the appliance, see "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 60. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 58.

Procedure

1 Download the zipped updated bundle from the VMware.com Web site.

2 On your chosen web server, create a repository directory under the document root: for example, `vc_update_repo`.

3 Extract the zipped bundle into the repository directory.

The extracted files are in two subdirectories: `manifest` and `package-pool`.

4 Open the management vCenter Virtual Appliance web interface on port 5480.

5 In the Update tab, click **Settings**.

6 Select **Use Specified Repository**.

7 For the Repository URL, enter the URL of the repository you created.

For example, if the repository directory is `vc_update_repo`, the URL should be similar to the following URL: `http://web_server_name.your_company.com/vc_update_repo`

8 Click **Save Settings**.

9 Click **Status**.

10 Under Actions, click **Install Updates**.

Update the VMware vCenter Server Appliance from the CD-ROM Drive

You can update the vCenter Server Appliance from an ISO file that the appliance reads from the virtual CD-ROM drive.

To update the vCenter Server Appliance from a zipped update bundle that you download to your own internal repository, see "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 59. To update the vCenter Server Appliance from a VMware public repository, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 58. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 58.

Procedure

1 Download the update ISO file from the VMware.com Web site.

2 Connect the vCenter Server Appliance CD-ROM drive to the ISO file you downloaded.

3 Open the management vCenter Virtual Appliance web interface on port 5480.

4 In the Update tab, click **Settings**.

5 Under Update Repository, select **Use CD-ROM Updates**.

6 Click **Save Settings**.

7 Click **Status**.

8 Under Actions, click **Install Updates**.

vCenter Server Upgrade Fails When Unable to Stop Tomcat Service

A vCenter Server upgrade can fail when the installer is unable to stop the Tomcat service.

Problem

If the vCenter Server installer cannot stop the Tomcat service during an upgrade, the upgrade fails with an error message similar to `Unable to delete VC Tomcat service`. This problem can occur even if you stop the Tomcat service manually before the upgrade, if some files that are used by the Tomcat process are locked.

Solution

1 From the Windows **Start** menu, select **Settings > Control Panel > Administrative Tools > Services**.

2 Right-click **VMware VirtualCenter Server** and select **Manual**.

3 Right-click **VMware vCenter Management Webservices** and select **Manual**.

4 Reboot the vCenter Server machine before upgrading.

This releases any locked files that are used by the Tomcat process, and enables the vCenter Server installer to stop the Tomcat service for the upgrade.

Solution

Alternatively, you can restart the vCenter Server machine and restart the upgrade process, but select the option not to overwrite the vCenter Server data.

After You Upgrade vCenter Server

After you upgrade to vCenter Server, consider the postupgrade options and requirements.

- To view the database upgrade log, open `%TEMP%\VCDatabaseUpgrade.log`.
- Install the vSphere Client and make sure that you can access the vCenter Server instance.

- Upgrade any additional modules that are linked to this instance of vCenter Server, such as vSphere Update Manager.
- On the VMware Web site, log in to your account page to access the license portal. From the license portal, upgrade your VirtualCenter 2.x or vCenter Server license. Using the vSphere Client, assign the upgraded license key to the vCenter Server 5.0 host.
- In the vSphere Client, select **Home > vCenter Server Settings > Licensing** to verify that the vCenter Server is connected to a license server. A license server is required if this vCenter Server is managing version 3.5 ESX or ESXi hosts. For information about installing the VMware License Server, see the documentation for VMware Infrastructure 3.
- For Oracle databases, copy the Oracle JDBC Driver (`ojdbc14.jar`) driver to the`[VMware vCenter Server]\tomcat\lib` folder.
- For SQL Server databases, if you enabled bulk logging for the upgrade, disable it after the upgrade is complete.
- Optionally, join the vCenter Server system to a Linked Mode group.
- Optionally, upgrade or migrate the ESXi or ESX hosts in the vCenter Server inventory to ESXi 5.0.
- If it is not enabled, enable SSL certification checking for all vSphere HA clusters. SSL certification checking is required to configure HA on the hosts. In vCenter Server, select **Administration > vCenter Server Settings > SSL Settings > vCenter requires verified host SSL certificates**. Follow the instructions to verify each host SSL certificate and click **OK**. If necessary, reconfigure HA on the hosts.

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.

Upgrade the vSphere Client

Virtual machine users and vCenter Server administrators must use the vSphere Client 5.0 to connect to vCenter Server 5.0 or to connect directly to ESX 5 hosts.

You can install the VI Client 2.5, the vSphere Client 4.x, and vSphere Client 5.0 on the same machine. After you upgrade vCenter Server, be sure to upgrade the vSphere Client to the same version to avoid compatibility problems that might interfere with the proper operation of the vSphere Client.

The vSphere Client upgrade operation requires no downtime. You do not need to power off virtual machines or clients.

Prerequisites

- Verify that you have the vCenter Server installer or 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 (Optional) Use **Add/Remove Programs** from the Windows Control Panel to remove any previous vCenter Server client.

You do not need to remove earlier versions of vCenter Server clients. These are useful if you need to connect to legacy hosts.

2 Run the vSphere Client installer.

- Start the vCenter Server installer. In the software installer directory, double-click the `autorun.exe` file and select **vSphere Client**.
- If you downloaded the vSphere Client, double-click the `VMware-viclient-`*`build number`*`.exe` file.

After you install the vSphere Client 5.0, you can connect to vCenter Server using the domain name or IP address of the Windows machine on which vCenter Server is installed and the user name and password of a user on that machine.

If you do not have the VI Client 2.5 installed and you use vSphere Client to connect to VirtualCenter 2.5, the vSphere Client prompts you to download and install the VI Client 2.5. After you install the VI Client 2.5, you can use the vSphere Client log-in interface to connect to VirtualCenter 2.5 or vCenter Server 5.0.

What to do next

Use the vSphere Client to connect to the vCenter Server IP address with your Windows login user name and password. Use the login credentials appropriate to the Windows machine on which vCenter Server is installed. The vCenter Server user name and password might be different than the user name and password you use for ESXi.

If the vSphere Client displays security alerts and exceptions when you log in or perform some operations, such as opening performance charts or viewing the **Summary** tab, this might mean that your Internet Explorer (IE) security settings are set to High. If your IE security settings are set to High, enable the **Allow scripting of Internet Explorer web browser control** setting in IE.

If you cannot connect to the vCenter Server system, you might need to start the VMware VirtualCenter Server service manually. To start the service, in the **Settings** menu, select **Control Panel > Administrative Tools > Services > VMware VirtualCenter Server**. The machine might require several minutes to start the service.

Using a License Server to Manage Version 3.5 ESX or ESXi Hosts

vCenter Server 5.0 requires a license server to manage ESX/ESXi version 3.5 hosts.

vCenter Server 5.0 does not require a license server to manage ESX or ESXi version 4.x hosts.

If you have a license server installed, you can configure your newly installed or upgraded vCenter Server to use the license server. If you do not have a license server installed, you can download the VMware License Server from the VMware Web site at http://downloads.vmware.com/d/details/esx_35_licenseserver_dt/dGViZGVoKmJkZXBo. After you have installed the license server, configure vCenter Server to use it.

See the information about configuring vCenter Server to use a license server in the *vCenter Server and Host Management* documentation.

You can also upgrade legacy hosts to manage them through vCenter Server without a license server.

License Server Upgrade Scenarios

If you upgrade to vCenter Server 5.0 and you want the vCenter Server system to manage version 3.5 ESX or ESXi hosts, verify that the license server is running and that vCenter Server 5.0 is configured to access the license server.

To configure vCenter Server to access a license server, see the *vCenter Server and Host Management* documentation.

Table 4-6. License Server Upgrade Scenarios

Upgrade Scenario	Action Required
Upgrade from VirtualCenter 2.x to vCenter Server 5.0. License server is on the same machine.	None
Upgrade from VirtualCenter 2.x to vCenter Server 5.0. License server is on a different machine.	None
Uninstall VirtualCenter 2.x. Preserve the license server. Perform a clean installation of vCenter Server 5.0 with a rebuilt, clean database.	Configure vCenter Server to access the existing license server.
Uninstall VirtualCenter 2.x and the license server. Perform a clean installation of vCenter Server 5.0 with a rebuilt, clean database.	Install a new license server, and configure vCenter Server to access the new license server.
Clean installation of vCenter Server 5.0 with a rebuilt, clean database. License server is on a different machine.	Configure vCenter Server to access the existing license server.
Upgrade to vCenter Server 5.0 using a different machine. The VirtualCenter 2.x system is the source machine. The vCenter Server 5.0 system is the destination machine. See "Upgrade to vCenter Server on a Different Machine and Upgrade the Database," on page 43.	Configure vCenter Server to access the existing license server.

Linked Mode Considerations for vCenter Server

Consider several issues before you configure a Linked Mode group.

Before you configure a Linked Mode group, consider the following issues.

- If you upgrade a vCenter Server that is part of a Linked Mode group, it will be removed from the group. vCenter Server does not support Linked Mode groups that contain both version 5.0 and earlier versions of vCenter Servers. After all vCenter Servers in the group are upgraded to version 5.0, you can rejoin them.
- Each vCenter Server user sees the vCenter Server instances on which they have valid permissions.
- When you set up your vCenter Server Linked Mode group, you must install the first vCenter Server as a standalone instance because you do not yet have a remote vCenter Server machine to join. Subsequent vCenter Server instances can join the first vCenter Server or other vCenter Server instances that have joined the Linked Mode group.
- If you join a vCenter Server to a standalone instance that is not part of a domain, you must add the standalone instance to a domain and add a domain user as an administrator.
- The vCenter Server instances in a Linked Mode group do not need to have the same domain user login. The instances can run under different domain accounts. By default, they run as the LocalSystem account of the machine on which they are running, which means that they are different accounts.
- During vCenter Server installation, if you enter an IP address for the remote instance of vCenter Server, the installer converts it into a fully qualified domain name.

- You cannot join a Linked Mode group during the upgrade procedure when you are upgrading from VirtualCenter 25 to vCenter Server 5.0. You can join after the upgrade to vCenter Server is complete.

CAUTION If you need to uninstall and reinstall vCenter Server on more than one member of a Linked Mode group, do so with a single vCenter Server at a time. Uninstalling and reinstalling multiple linked vCenter Servers at the same time is not supported, and can cause errors that prevent vCenter Server from connecting to vCenter Inventory Service. If it is necessary to uninstall and reinstall multiple linked vCenter Servers at the same time, isolate them from the Linked Mode group first, and rejoin them to the Linked Mode group after the reinstallation is complete.

Linked Mode Prerequisites for vCenter Server

Prepare the vCenter Server system for joining a Linked Mode group.

Before joining a vCenter Server to a Linked Mode group, review "Linked Mode Considerations for vCenter Server," on page 63.

All the requirements for standalone vCenter Server systems apply to Linked Mode systems.

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

- Linked Mode groups that contain both vCenter Server 5.0 and earlier versions of vCenter Server are not supported. The vSphere Client does not function correctly with vCenter Servers in groups that have both version 5.0 and earlier versions of vCenter Server. Do not join a version 5.0 vCenter Server to earlier versions of vCenter Server, or an earlier version of vCenter Server to a version 5.0 vCenter Server. Upgrade any vCenter Server instance to version 5.0 before joining it to a version 5.0 vCenter Server.
- To join a Linked Mode group the vCenter Server must be in evaluation mode or licensed as a Standard edition. vCenter Server Foundation and vCenter Server Essentials editions do not support Linked Mode.
- DNS must be operational for Linked Mode replication to work.
- The vCenter Server instances in a Linked Mode group can be in different domains if the domains have a two-way trust relationship. Each domain must trust the other domains on which vCenter Server instances are installed.
- When adding a vCenter Server instance to a Linked Mode group, the installer must be run by a domain user who is an administrator on both the machine where vCenter Server is installed and the target machine of the Linked Mode group.
- All vCenter Server instances must have network time synchronization. The vCenter Server installer validates that the machine clocks are not more than five minutes apart.

Join a Linked Mode Group After a vCenter Server Upgrade

After you upgrade to vCenter Server 5.0, you can join the system to a Linked Mode group. A Linked Mode group allows you to log in to any single instance of vCenter Server in the group and view and manage the inventories of all the vCenter Server systems in the group.

Prerequisites

See "Linked Mode Prerequisites for vCenter Server," on page 64.

NOTE Joining a version 5.0 vCenter Server to older versions of vCenter Server is not supported.

Procedure

1 From the **Start** menu, select **All Programs > VMware > vCenter Server Linked Mode Configuration**.

2 Click **Next**.

3 Select **Modify linked mode configuration** and click **Next**.

4 Click **Join vCenter Server instance to an existing linked mode group or another instance** and click **Next**.

5 Type the server name and LDAP port number of any remote vCenter Server that is or will be a member of the group and click **Next**.

If you enter an IP address, the installer converts it to a fully qualified domain name.

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

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

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

7 Click **Finish**.

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

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

After you form a Linked Mode group, you can log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Servers in the group.

What to do next

For information about Linked Mode groups, see the *vCenter Server and Host Management* documentation.

Set the Maximum Number of Database Connections After a vCenter Server Upgrade

By default, a vCenter Server creates a maximum of 50 simultaneous database connections. If you configure this value to less than 50 in the previous version of vCenter Server and then perform the upgrade to vCenter Server 5.0, the upgrade restores the default setting of 50. If you configure this value to more than 50 in the previous version of vCenter Server, after the upgrade to vCenter Server 5.0, the system retains the previous value. You can reconfigure the nondefault setting.

You might want to increase the number of database connections if the vCenter Server frequently performs many operations and performance is critical. You might want to decrease this number if the database is shared and connections to the database are costly. Do not change this value unless your system has one of these problems.

Perform this task before you configure the authentication for your database. For more information about configuring authentication, see the documentation for your database.

Procedure

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

2 Click **Database**.

3 In the **Current vCenter Server** menu, select the appropriate server.

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

5 Restart the vCenter Server.

The new database setting takes effect.

Restore VirtualCenter or vCenter Server

You can restore the previous VirtualCenter or vCenter Server configurations if you have a full backup of your VirtualCenter or vCenter database and the previous VirtualCenter and vCenter SSL certificates.

Prerequisites

Iin the event of a system failure or disaster, you might need some or all of the following items to restore VirtualCenter and its components. Follow your company disaster recovery guidelines for storage and handling of these items.

- Installation media for the same version of VirtualCenter that you are restoring.
- VMware Infrastructure 3 license file or a running license server when you are restoring VirtualCenter 2.5.
- Database backup files.
- SSL files found in: `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter\SSL` on the VirtualCenter or vCenter systems.
- Notes from the original installation regarding the selections, settings, and information used.
- `vpxd.cfg` files.
- vCenter Server and ESX/ESXi license keys.

Procedure

1 Uninstall the VirtualCenter or the vCenter Server.

2 Restore the previous version of the VirtualCenter or vCenter Server database from the backup.

See your database documentation.

3 Reinstall your original version of VirtualCenter or vCenter Server, selecting the restored database during the installation process.

4 Verify that the license server is running if one was in use in the original installation.

5 Restore the VirtualCenter SSL certificate folder and `vpxd.cfg` to the `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter` directory.

6 Make sure the system DSN points to the database.

Upgrading Datastore and Network Permissions

In previous releases of vCenter Server, datastores and networks inherited access permissions from the datacenter. In vCenter Server 4.0 and later, datastores and networks have their own set of privileges that control access to them. You might have toassign privileges manually, depending on the access level you require.

In vCenter Server 5.0, users are granted the No Access role on all new managed objects, including datastores and networks. This means, by default, users cannot view or perform operations on them. All existing objects in vCenter Server maintain their permissions after the upgrade. To determine whether to assign permissions to existing datastores and networks, the upgrade process uses the datacenter's **Read-only** privilege.

- **Read-only** privilege is nonpropagating (not inherited by child objects). VMware assumes that access privileges should not be assigned to datastores and networks. You must update your roles to include the new datastore and network privileges. These privileges are required for users to view and perform operations on these objects.
- **Read-only** privilege is propagating (inherited by child objects). VMware assumes that access privileges should be assigned to datastores and networks so that users can view them and perform basic operations that require access. The default minimum privileges are assigned during the upgrade process.

  After the upgrade process, if your roles require users to have more privileges, for example, the ability to delete a datastore or network, update your permission roles.

Table 4-7. Datastore and Network Permission Requirements

Object	Before Upgrade Privilege	After Upgrade Privilege	Action Required to Enable Access
Datastore	Nonpropagating Read-only	No Access	Assign access privileges for datastores or datastore folders.
	Propagating Read-only	**Allocate Space**	None.
Network	Nonpropagating Read-only	No Access	Assign access privileges for networks or network folders.
	Propagating Read-only	**Assign Network**	None.

NOTE The **Read-only** propagating permission on a datacenter, as well as all other permissions you have set, will continue to work as expected after the upgrade.

Datastore Privileges

In VMware vSphere 5.0, datastores have their own set of access control privileges. As a result, you might need to reconfigure your permissions to grant the new datastore privileges. This is required if you have nonpropagating **Read-only** permission set on the datacenter for users.

Table 4-8. Datastore Privileges

Privilege Name	Actions Granted to Users	Affects	Pair with Object	Effective on Object
Allocate Space	Allocate space on a datastore for a virtual machine, snapshot, or clone.	hosts, vCenter Servers	datastores	datastores, virtual disks
Browse Datastore	Browse files on a datastore, including CD-ROM or Floppy media and serial or parallel port files. In addition, the browse datastore privilege allows users to add existing disks to a datastore.	hosts, vCenter Servers	datastores	datastores, datastore folders, hosts, virtual machines
Delete Datastore	Remove a datastore.	hosts, vCenter Servers	datastores	datastores, datastore folders

Table 4-8. Datastore Privileges (Continued)

Privilege Name	Actions Granted to Users	Affects	Pair with Object	Effective on Object
Delete Datastore File	Delete a file in the datastore.	hosts, vCenter Servers	datastores	datastores
File Management	Carry out file operations in the datastore browser.	hosts, vCenter Servers	datastores	datastores
Move Datastore	Move a datastore between folders in the inventory. NOTE Privileges are required on both the source and destination objects.	vCenter Servers	datastore, source and destination object	datastores, datastore folders
Rename Datastore	Rename a datastore.	hosts, vCenter Servers	datastores	datastores

Update Datastore Permissions

You must change **Read-only** nonpropagating datastore permissions to propagating datastore permissions in order for users to access the datastores. You can assign datastore permissions on datastores or folders containing datastores.

Prerequisites

Before performing the upgrade procedure, determine which users need access to each datastore and which privileges each user needs. If necessary, define new datastore roles or modify the **Database Consumer** sample role. This sample role assigns the **Allocate Space** privilege to the datastore, which enables users to perform basic virtual machine operations, such as creating clones and taking snapshots. In addition, organize your datastores in folders that coincide with users' access needs.

NOTE The **Read-only** propagating permission on a datacenter, in addition to all permissions you have set, will be kept intact after the datastore permissions upgrade.

Procedure

1 Log in to vSphere Client as an administrator.

2 On the Home page, click **Datastores** to display the datastores in the inventory.

3 Select the datastore or datastore folder and click the **Permissions** tab.

4 Right-click in the **Permissions** tab and from the context pop-up menu, choose **Add Permission**.

5 In the **Assigned Role** pane, assign a role.

- To assign specific datastore privileges defined in a role by your company, choose the custom role.
- To migrate read-only nonpropagating datacenter permissions to propagating datastore permissions, choose **Datastore Consumer (sample)**. This role assigns the **Allocate Space** privilege to users, which is required so that users can consume space on the datastores on which this role is granted. In order to perform a space-consuming operation, such as creating a virtual disk or taking a snapshot, the user must also have the appropriate virtual machine privileges granted for these operations.
- To assign **Read-only** datastore privileges, choose **Read-only**.

  This role enables users to browse the datastore without giving them other datastore privileges. For example, choose **Read-only** for users who need to attach CD/DVD-ROM ISO images to a datastore.

6 Select **Propagate to Child Objects**.

7 In the Users and Groups pane, click **Add**.

8 Select the users and groups for whom to add the role.

To select multiple names, control-click each additional name.

9 Click **OK**.

All users are added to the **Users and Groups** list for this role.

10 Click **OK**.

The datastore is saved with the new permissions.

NOTE You need to set up permissions for new datastores that you create. By default, new datastores are created under the datacenter folder in the inventory. You can move it into a datastore folder, as appropriate.

Network Privileges

In VMware vSphere 4.0 and higher, networks have their own set of access control privileges. As a result, you might need to reconfigure your permissions to grant the new network privileges. This is required if you have nonpropagating **Read-only** permission set on the datacenter.

Table 4-9 lists the default network privileges that, when selected for a role, can be paired with a user and assigned to a network.

Table 4-9. Network Privileges

Privilege Name	Actions Granted to Users	Affects	Pair with Object	Effective on Object
Assign Network	Assign a network to a virtual machine.	VCenter Servers	virtual machine	network, virtual machine
Configure Network	Configure a network.	hosts, vCenter Servers	network, network folder	networks, virtual machines
Delete Network	Remove a network.	hosts, vCenter Servers	datacenter	datacenters
Move Network	Move a network between folders in the inventory. **NOTE** Privileges are required on both the source and destination objects.	hosts, vCenter Servers	network, source and destination	networks

Update Network Permissions

You must change **Read-only** nonpropagating network permissions to propagating network permissions in order for users to access the networks. You can assign network permissions on networks or folders containing networks.

Before performing the update procedure, determine the network organization for virtual machines, hosts, and users. If necessary, define new networking roles or modify the **Network Consumer** sample role. This sample role assigns the **Assign Network** privilege. In addition, group your networks in folders that coincide with your organizational needs.

NOTE The **Read-only** propagating permission on a datacenter, in addition to all permissions you have set, will be kept intact after the network permissions upgrade.

Procedure

1 Log in to vSphere Client as an administrator.

2 On the Home page, click **Networking** to display the networks in the inventory.

3 Select the network or network folder and click the **Permissions** tab.

4 Right-click in the **Permissions** tab and from the context menu, choose **Add Permission**.

5 In the **Assigned Role** pane, do one of the following:

- To assign specific network privileges defined in a role by your company, choose the custom role.

  NOTE The **Read-only** propagating permission on a datacenter, in addition to all permissions you have set, will be kept intact after the upgrade.

- To migrate read-only nonpropagating datacenter permissions to propagating network permissions, choose **Network Consumer (sample)**. This role assigns the **Assign Network**privilege to users, which is required so that users can associate a virtual machine's vNIC or host's NIC with the network on which this role is granted. This requires the appropriate permissions for the assignment are also granted on the virtual machines or hosts.

6 Select **Propagate to Child Objects**.

7 In the **Users and Groups** pane, click **Add**.

8 Select the users and groups for whom to add the role.

  To select multiple names, control-click each additional name.

9 Click **OK**.

  All users are added to the **Users and Groups** list for this role.

10 Click **OK**.

New networks that you create are added under the datacenter by default.

NOTE You need to set up permissions for new networks that you create. By default, new networks are created under the datacenter folder in the inventory. You can move it into a network folder, as appropriate.

Upgrading Update Manager 5

You can upgrade Update Manager 1.0 Update 6 and Update Manager 4.x to Update Manager 5.0.

You can install Update Manager 5.0 only on a 64-bit operating system. If you are running an earlier version of Update Manager on a 32-bit platform, you must either back up and restore your database manually, or use the data migration tool to back up the existing data on the 32-bit machine, and then restore your data on the 64-bit machine on which you are installing Update Manager 5.0.

When you upgrade Update Manager, you cannot change the installation path and patch download location. To change these parameters, you must install a new version of Update Manager rather than upgrade.

Previous versions of Update Manager use a 512-bit key and self-signed certificate and these are not replaced during upgrade. If you require a more secure 2048-bit key, you can either perform a fresh installation of Update Manager 5.0, or use the Update Manager Utility to replace the existing certificate.

Scheduled tasks for virtual machine patch scan and remediation are not removed during the upgrade. After the upgrade, you can edit and remove scheduled scan tasks that exist from previous releases. You can remove existing scheduled remediation tasks but you cannot edit them.

Virtual machine patch baselines are removed during the upgrade. Existing scheduled tasks that contain them run normally and ignore only the scanning and remediation operations that use virtual machine patch baselines.

You must upgrade the Update Manager database during the Update Manager upgrade. You can select whether to keep your existing data in the database or to replace it during the upgrade.

This chapter includes the following topics:

- "Upgrade the Update Manager Server," on page 71
- "Upgrade the Update Manager Client Plug-In," on page 73

Upgrade the Update Manager Server

To upgrade an instance of Update Manager that is installed on a 64-bit machine, you must first upgrade vCenter Server to a compatible version.

The Update Manager 5.0 release allows upgrades from Update Manager 1.0 Update 6 and Update Manager 4.x.

Prerequisites

- Ensure that you grant the database user the required set of privileges. See the *Preparing the Update Manager Database* chapter in *Installing and Administering VMware vSphere Update Manager*.
- Stop the Update Manager service and back up the Update Manager database. The installer upgrades the database schema, making the database irreversibly incompatible with previous Update Manager versions.

Procedure

1 Upgrade vCenter Server to a compatible version.

NOTE The vCenter Server installation wizard warns you that Update Manager is not compatible when vCenter Server is upgraded.

If prompted, you must restart the machine that is running vCenter Server. Otherwise, you might not be able to upgrade Update Manager.

2 In the software installer directory, double-click the `autorun.exe` file at `C:\installer_location`, and select **vSphere Update Manager**.

If you cannot launch the `autorun.exe` file, browse to locate the `UpdateManager` folder and run `VMware-UpdateManager.exe`.

3 Select a language and click **OK**.

4 In the upgrade warning message, click **OK**.

5 Review the Welcome page and click **Next**.

6 Read the patent agreement and click **Next**.

7 Accept the terms in the license agreement and click **Next**.

8 Review the support information, select whether to delete old upgrade files, select whether to download updates from the default download sources immediately after installation, and click **Next**.

If you deselect **Delete the old host upgrade files from the repository**, you retain files that you cannot use with Update Manager 5.0.

If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click **Download Now** on the Download Settings page. You can modify the default download schedule after the installation is complete.

9 Type the vCenter Server system credentials and click **Next**.

To keep the Update Manager registration with the original vCenter Server system valid, keep the vCenter Server system IP address and enter the credentials from the original installation.

10 Type the database password for the Update Manager database and click **Next**.

The database password is required only if the DSN does not use Windows NT authentication.

11 On the Database Upgrade page, select **Yes, I want to upgrade my Update Manager database** and **I have taken a backup of the existing Update Manager database**, and click **Next**.

12 (Optional) On the Database re-initialization warning page, select to keep your existing remote database if it is already upgraded to the latest schema.

If you replace your existing database with an empty one, you lose all of your existing data.

13 Specify the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

Configure the proxy settings if the computer on which Update Manager is installed has access to the Internet.

14 (Optional) Provide information about the proxy server and port, specify whether the proxy should be authenticated, and click **Next**.

15 Click **Install** to begin the upgrade.

16 Click **Finish**.

You upgraded the Update Manager server.

What to do next

Upgrade the Update Manager Client plug-in.

Upgrade the Update Manager Client Plug-In

The Update Manager server and the Update Manager Client plug-in must be of the same version.

Prerequisites

Upgrade the Update Manager server.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered.

2 Select **Plug-ins > Manage Plug-ins**.

3 In the Plug-in Manager window, click **Download and install** for the VMware vSphere Update Manager extension.

4 Complete the Update Manager Client installation, and click **Finish**.

The status for the Update Manager extension is displayed as Enabled.

5 Click **Close** to close the Plug-in Manager window.

The icon for the Update Manager Client plug-in is displayed on the vSphere Client Home page.

Upgrading and Migrating Your Hosts 6

After you upgrade vCenter Server, and vSphere Update Manager if you are using Update Manager, upgrade or migrate VMware ESX 4.x and ESXi 4.x hosts to ESXi 5.0.

These topics are intended for administrators who are upgrading ESX, ESXi, and virtual machines from ESX 4.x/ESXi 4.x to ESXi 5.0.

This chapter includes the following topics:

- "Preparing to Upgrade Hosts," on page 75
- "Performing the Upgrade or Migration," on page 96
- "After You Upgrade or Migrate Hosts," on page 141

Preparing to Upgrade Hosts

For a successful upgrade of your hosts, understand and prepare for the changes that are involved.

Best Practices for ESXi Upgrades and Migrations

When you upgrade or migrate hosts, you must understand and follow the best practices process for a successful upgrade or migration.

For a successful upgrade or migration, follow these best practices:

1. Make sure that you understand the ESXi upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.
   - If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Read "Preparing to Upgrade Hosts," on page 75 to understand the changes in configuration and partitioning between ESXi 4.x and ESXi 4.x and ESXi 5.0, the upgrade and migration scenarios that are supported, and the options and tools available to perform the upgrade or migration.
   - Read the VMware vSphere 5.0 Release Notes for known installation issues.
   - If your vSphere installation is in a VMware View environment, see "Upgrading vSphere Components Separately in a VMware View Environment," on page 171.
2. Prepare your system for the upgrade.
   - Make sure your current ESX or ESXi version is supported for migration or upgrade. See "Supported Upgrades and Updates to ESXi 5.0.x," on page 84.

- Make sure your system hardware complies with ESXI 5.0 requirements. See Chapter 3, "System Requirements," on page 13 and the VMware Compatibility Guide, at http://www.vmware.com/resources/compatibility/search.php. Check for system compatibility, I/O compatibility (network and HBA cards), storage compatibility, and backup software compatibility.

  Server hardware for ESXi 5.0 must be 64-bit compatible. Intel VT must be enabled in the host BIOS.

- Make sure that sufficient disk space is available on the host for the upgrade or migration. Migrating from ESX 4.x to ESXi 5.0 requires 50MB of free space on your VMFS datastore.

- If a SAN is connected to the host, detach the fibre before continuing with the upgrade or migration. Do not disable HBA cards in the BIOS.

  NOTE This step does not apply to ESX hosts that boot from the SAN and have the Service Console on the on the SAN LUNs. You can disconnect LUNs that contain the VMFS datastore and do not contain the Service Console.

3 Back up your host before performing an upgrade or migration, so that, if the upgrade fails, you can restore your 4.x host.

  IMPORTANT Once you have upgraded or migrated your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software.

4 Depending on the upgrade or migration method you choose, you might need to migrate or power off all virtual machines on the host. See the instructions for your upgrade or migration method.

5 After the upgrade or migration, test the system to ensure that the upgrade or migration completed successfully.

6 Reapply your host licenses. See "Reapplying Licenses After Upgrading to ESXi 5.0," on page 142.

7 Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. Optionally, you can install the vSphere Syslog Collector to collect logs from all hosts. See "Providing Sufficient Space for System Logging," on page 21. For information about setting up and configuring syslog and a syslog server, setting up syslog from the host profiles interface, and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

8 If the upgrade or migration was unsuccessful, and you backed up your version 4.x host, you can restore your host.

Files and Configuration Settings Affected by the Migration or Upgrade to ESXi 5.0

The migration or upgrade from ESX 4.x or ESXi 4.x to ESXi 5.0 does not migrate all host configuration files and settings.

After the upgrade, you must reconfigure some host settings.

Migrating ESX 4.x Files and Settings to ESXi 5.0

The upgrade process preserves as much of the ESX host configuration as possible. However, because of the architectural differences between ESX 4.x and ESXi 5.0 architecture, many configuration files cannot be migrated when you select the **Migrate** option in the ESXi installation or upgrade wizard.

Pertinent VMware files, such as `/etc/vmware/esx.conf` are migrated, but many existing settings such as third-party agents and scripts, cannot be migrated.

NOTE If a host contains customizations, such as third-party VIBS or drivers, upgrading with the standard VMware installer ISO will result in the loss of those customizations, and possibly an unstable system. Use ESXi Image Builder CLI to create a customized ESXi installer ISO file that includes the VIBs or drivers. See the information on Image Builder in the *vSphere Installation and Setup* documentation.

Table 6-1. Files Migrated During Migration or Upgrade to ESXi

File Migrated	Comments
/etc/sfcb/sfcb.cfg	Migrated.
/var/lib/sfcb/registration/repository/root/interop/*	Migrated.
/etc/logrotate.conf	Not migrated. ESXi Logrotation is incompatible with prior versions.
/etc/localtime	Not migrated. Timezones are not supported in ESXi.
/etc/ntp.conf	Migrated.
/etc/ntp.drift	Migrated.
/etc/ntp.keys	Migrated.
/etc/syslog.conf	Migrated for ESXi, not migrated for ESX.
/etc/security/access.conf	Migrated. Needed for PAM configurations.
/etc/security/login.map	
/etc/sysconfig/network	Migrated. Service Console virtual NICs (vswifs) will be converted to ESXi virtual NICs. (vmks)
/etc/sysconfig/ntp	Not migrated.
/etc/sysconfig/xinetd	Not migrated.
/etc/sysconfig/console/*	Not migrated.
/etc/sysconfig/i18n	Not migrated. i18n is not supported in ESXi
/etc/sysconfig/clock	Not migrated. Timezones are not supported in ESXi.
/etc/sysconfig/crond	Not migrated.
/etc/sysconfig/syslog	Not migrated. The syslog daemon is incompatible with prior versions.
/etc/sysconfig/keyboard	Migrated. Any entries not supported will default to English.
/etc/sysconfig/mouse	Not migrated. No mouse support in ESXi.
/etc/sysconfig/static-routes	Migrated.
/etc/sysconfig/static-routes-ipv6	Migrated.
/etc/sysconfig/network-scripts/route-$device	Migrated.
/etc/ssh	Not migrated.
/etc/nsswitch.conf	Migrated. Used generically for various configurations, most helpful for Active Directory authentication.
/etc/yp.conf	Not migrated. NIS is not supported in ESXi.
/etc/krb.conf	Needed for Likewise to have Active Directory support.
/etc/krb.realms	
/etc/krb5.conf	
/etc/krb5.acl	
/etc/krb5.keytab	
/etc/krb5.log	
/etc/krb5.mkey	
/etc/login.defs	Not migrated. This file controls settings like maildir, password aging controls, uid and gid min/max settings, and the user deletion command.

Table 6-1. Files Migrated During Migration or Upgrade to ESXi (Continued)

File Migrated	Comments
/etc/pam.d/*	Partially migrated. Needed for authentication and authorization. **NOTE** Custom edits made to settings in /etc/pam.d/system–auth in ESX 4.x are reset to the default values by the upgrade to ESXi 5.0. To maintain the custom values, reset them manually after the upgrade.
/etc/hosts.allow	Not migrated.
/etc/hosts.deny	Not migrated.
/etc/ldap.conf	Not migrated. LDAP is not supported in ESXi.
/etc/openldap	
/etc/sudoers	Not migrated. SUDO is not supported in ESXi.
/etc/snmp/snmpd.conf	Migrated to /etc/vmware/snmp.xml.
/usr/local/etc/	Not migrated.
/etc/rc.d/rc*.d/*	Not migrated. ESX and ESXi rc.d scripts are incompatible.
/etc/xinetd.conf	Not migrated. xinetd is not supported in ESXi.
/etc/motd	Migrated. A note is appended saying the system was upgraded to ESX 5.x
/etc/likewise/*	Migrated. Used for Likewise configurations.
/etc/vmware/vmkiscsid/*	Migrated.
etc/vmware/init/*	Not migrated. Init scripts are incompatible.
/etc/vmware/esx.conf	Migrated.
/etc/vmware/pci*	Not migrated.
/etc/vmware/simple.map	Not migrated. A new simple.map file is generated.
/etc/vmware/license.cfg	Not migrated. The valuation mode timer is be reset on upgrades.
/etc/vmware/vmware.lic	Not migrated. ESXi 5.0 upgrades are reset to evaluation mode.
/etc/vmware/hostd/*	Migrated.
/etc/vmware/hostd/config.xml	Not migrated. This file is currently incompatible with ESXi.
/etc/vmware/hostd/proxy.xml	Not migrated. This file is currently incompatible with ESXi.
/etc/vmware/vmauth/authentication.conf	Migrated. Used for Likewise configurations.
/etc/vmware/vmauth/provider.xml	
/etc/hosts	Migrated.
/etc/resolv.conf	Migrated.
/usr/lib/vmware	Not migrated.
/etc/fstab	Partially migrated. Only NFS entries will be migrated to ESXi.
/etc/passwd	Partially migrated. Only the root user password will be saved, if possible.
/etc/shadow	
/etc/groups	Not migrated.

Firewall Configuration Changes After Migration or Upgrade to ESXi 5.0

The migration or upgrade from ESX/ESXi 4.x to ESXi 5.0 results in several changes to the host firewall configuration.

When you migrate from ESX 4.x to ESXi 5.0, the ESX 4.x rulesets list is replaced by the new rulesets list in ESXi 5.0. The following configuration from the `/etc/vmware/esx.conf` file is preserved:

- The existing enabled/disabled status.
- The allowedip added by `esxcfg-firewall`.

Ruleset files that are added by the user and customized firewall rules created in ESX 4.x. are not preserved after the migration. In the first boot after the migration, for those rulesets that don't have entries in the ESX 4.x `/etc/vmware/esx.conf` file, the ESXi 5.0 firewall loads the default enabled status.

After the migration to ESXi 5.0, the default block policy is set to false (PASS all traffic by default) on ESXi 5.0 only when both blockIncoming and blockOutgoing values of the default policy are false in the ESX 4.x `/etc/vmware/esx.conf` file. Otherwise the default policy is to deny all traffic.

Custom ports that were opened by using the ESX/ESXi 4.1 `esxcfg-firewall` command do not remain open after the upgrade to ESXi 5.0. The configuration entries are ported to the `esx.conf` file by the upgrade, but the corresponding ports are not opened. See the information about ESXi firewall configuration in the *vSphere Security* documentation.

Important The ESXi firewall in ESXi 5.0 does not allow per-network filtering of vMotion traffic. Therefore, you must install rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket.

Resource Pool Settings Affected by the Upgrade from ESX 4.x to ESXi 5.0

After the upgrade to ESXi 5.0, ESX 4.x resource pool settings might be insufficient to start all virtual machines in the pool.

The upgrade to ESXi 5.0 affects the amount of memory available to the host system. As a result, in resource pools that are set to use nearly all of the resources available, some virtual machines might not have enough resources to start after the upgrade. When this happens, a system alert will be issued. You can find this alert by pressing Alt + F11 in the ESXi direct console. Reconfigure the resource pools to solve the problem.

SSH Configuration Affected by Upgrading or Migrating to ESXi 5.0

The host SSH configuration is migrated only for upgrades from ESXi 4.1 to ESXi 5.0

SSH configuration is not migrated for ESX 4.x hosts or ESXi 4.0 hosts. For these hosts, SSH access is disabled during the upgrade or migration process. You can reenable SSH access in the direct console. See the information on enabling SSH access in the *vSphere Installation and Setup* documentation.

Networking Changes in ESXi 5.0

Some ESX 4.x and ESXi 4.x network settings stored in `/etc/sysconfig/network` are migrated in the upgrade or migration to ESXi 5.0. In the migration to ESXi 5.0, ESX Service Console virtual NICs (vswifs) are converted to ESXi virtual NICs (vmks).

The distributed port group or dvPort that the virtual NICs connect to is also migrated. The Service Console port group is renamed as the Management Network port group. When vswifs are migrated to vmks, they are numbered to follow any existing vmk in sequence. For example, if the version 4.x ESX host has virtual NICs vmk0, vmk1, and vswif0, after the migration the new ESXi configuration will be vmk0, vmk1, and vmk2, where vmk2 is the management interface.

When virtual NICs are configured to use DHCP, a setting controls whether DHCP sets the default route and host name in addition to installing an IPv4 address. In ESX this setting is PEERDNS. In ESXi, the setting is DhcpDNS. The PEERDNS value for ESX Service Console virtual NICs is migrated to the DhcpDNS setting for the ESXi virtual NICs. The DhcpDNS setting preserves the ESX configuration for default route and host name as well as the IPv4 address.

The migration from ESX 4.x to ESXi 5.0 also preserves manually assigned IPv4 and IPv6 addresses, default route, and host-specific IPv4 and IPv6 routes.

When you upgrade from ESXi 4.x to ESXi 5.x, the default maximum number of ports for a virtual switch changes from 64 to 128. To keep the same maximum number of ports that you have in ESXi 4.x, set the value explicitly before you upgrade, using the vSphere Client.

ESX hosts have two IP stacks, one for the vmkernel and one for the Service Console. Because ESXi hosts have only one IP stack, the migration cannot preserve both ESX default routes. After migration, the ESX Service Console default route becomes the single ESXi default route, replacing the vmkernel route. The change to a single ESXi default route might cause loss of connectivity for routed nonmanagement traffic that originates from vmkernel. To restore vmkernel networking, you can configure static routes in addition to the default route.

All vswif interfaces are migrated to vmk interfaces. If a conflict is detected between two interfaces, one is left in disabled state. The upgrade disables any conflicting kernel IP addressing in favor of the management interface.

The migration to ESXi 5.0 disables any existing vmk virtual NIC that meets the following conditions.

- The vmk virtual NIC has a manually configured (static) IP address.
- The IP address is in the same subnet as a vswif virtual NIC that is being migrated to a switch containing the vmk virtual NIC.
- The vmk and vswif NICs are both on the same virtual switch.

For example, if vswif0, with IP address 192.0.2.1/24 on vswitch1, is migrated to a switch containing vmk0, with IP address 192.0.2.2/24, also on vswitch1, after the migration, vmk0 will be disabled.

ESX 4.x Service Console Port Group Removed in Migration to ESXi 5.0

Because ESXi 5.0 has no Service Console, migrating from ESX 4.x to ESXi 5.0 removes the Service Console port group.

After the migration to ESXi 5.0, a new port group, the Management Network port group, is created.

If any of your ESX hosts require the Service Console port group to support an existing service, you can write a firstboot script to recreate the port group after the migration. See the information on the `%firstboot` command in "Installation and Upgrade Script Commands," on page 114.

Partitioning Changes from ESX 4.x to ESXi 5.0

The ESXi partition scheme used in ESXi 5.0 differs from that of earlier ESX and ESXi versions. ESXi 5.0 does not have the Service Console partition found in ESX.

How these changes affect your host depends on whether you are upgrading to ESXi 5.0 or performing a fresh installation.

Partitioning in New ESXi 5.0 Installations

In new installations, several new partitions are created for the boot banks, the scratch partition, and the locker. New ESXi 5.0 installations use GUID Partition Tables (GPT) instead of MSDOS-based partitioning.

The partition table is fixed as part of the binary image, and is written to the disk at the time the system is installed. The ESXi installer leaves the scratch and VMFS partitions blank, and ESXi creates them when the host is rebooted for the first time after installation or upgrade. The scratch partition is 4GB. The rest of the disk is formatted as a VMFS5 partition.

NOTE The installer can create multiple VFAT partitions. The VFAT designation does not always indicate that the partition is a scratch partition. In some cases, a VFAT partition can lie idle.

Partitioning in Upgraded ESXi 5.0 Hosts

Upgraded systems do not use GUID Partition Tables (GPT), but retain the older MSDOS-based partition label.

For most ESXi 4.x hosts, the partition table is not rewritten in the upgrade to ESXi 5.0. The partition table is rewritten for systems that have lopsided bootbanks. Lopsided boot banks can occur in systems that are upgraded from ESXi 3.5 to ESXi 4.x, and then upgraded directly to ESXi 5.0.

For ESX hosts, the partitioning structure is changed to resemble that of an ESXi 4.x host. The VMFS3 partition is retained and a new MSDOS-based partition table overwrites the existing partition table.

For ESX hosts, any data stored in custom user created partitions inside the Service Console is not preserved in the migration to ESXi 5.0.

Upgraded hosts do not have a scratch partition. Instead, the scratch directory is created and accessed off of the VMFS volume. Each of the other partitions, such as the bootbanks, locker and vmkcore are identical to that of any other system.

In upgraded hosts, the VMFS partition is not upgraded from VMFS3 to VMFS5. ESXi 5.0 is compatible with VMFS3 partitions. You can upgrade the partition to VMFS5 after the host is upgraded to ESXi 5.0. See the information on upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Upgraded hosts, which keep the older MSDOS-based partitioning, do not support installing ESXi on a single physical disk or LUN larger than 2TB. To install ESXi on a disk or LUN larger than 2TB, you must do a fresh installation.

NOTE The ESXi 5.0 installer cannot detect ESX 2.x instances or VMFS2 datastores. You cannot migrate ESX 2.x instances to ESXi 5.0 or preserve VMFS2 datastores in an upgrade to ESXi 5.0. Instead, perform a fresh installation of ESXi 5.0.

For the VMFS partition on the disk to be preserved during an upgrade to ESXi 5.0, the partition must be physically located after the boot partition, which is partition 4, and the extended partition on the disk (8192 + 1835008 sectors). Any system that has a VMFS partition after the 1843200 sector mark can keep that VMFS partition, regardless of whether it was initially installed with ESX 3.5 or 4.x.

For systems in which the VMFS partition is placed on a different drive from the boot drive, the entire contents of the boot drive is overwritten during the upgrade. Any extra data on the disk is erased.

ESXi 5.0.x Upgrade and Update Options

VMware provides several ways to upgrade and update ESX/ESXi hosts.

vSphere Update Manager

vSphere Update Manager is software for upgrading, migrating, updating, and patching clustered hosts, virtual machines, and guest operating systems. Update Manager orchestrates host and virtual machine upgrades. If your site uses vCenter Server, VMware recommends that you use Update Manager. For instructions about conducting an orchestrated host upgrade, see "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 96. For instructions about conducting an orchestrated virtual machine upgrade, see "Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager," on page 147. For complete documentation about Update Manager, see the *Installing and Administering VMware vSphere Update Manager*.

Update, Upgrade or migrate interactively using an ESXi installer ISO image on CD/DVD or USB flash drive

You can run the ESXi 5.0.x installer from a CD/DVD or USB flash drive to do an interactive upgrade or migration. This method is appropriate for deployments with a small number of hosts. The installer works the same as for a fresh installation, but if you select a target disk that already contains an ESX/ESXi 4.x or ESXi 5.0 installation, the installer upgrades or updates the host to 5.0.x, and gives you the option to migrate some existing host settings and configuration files, and preserve the existing VMFS datastore. See "Upgrade or Migrate Hosts Interactively," on page 110.

Perform a scripted upgrade or update

You can upgrade or migrate hosts from version 4.x ESXi and ESX and update version 5.0 ESXi hosts to ESXi 5.0.x by invoking a script, for an efficient, unattended upgrade. Scripted upgrades and updates provide an efficient way to deploy multiple hosts. You can use a script to upgrade or update ESXi from a CD, DVD or USB flash drive, or by PXE-booting the installer. You can also call a script from an interactive installation. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 111.

vSphere Auto Deploy

Auto Deploy is a new feature in vSphere 5.0. Working with hosts managed by vCenter Server, Auto Deploy loads the ESXi image directly into the host memory, rather than installing it on the host hard disk. You cannot use Auto Deploy to upgrade or migrate version 4.x ESX and ESXi hosts to ESXi 5.0, because version 4.x ESX and ESXi hosts are deployed by the traditional method of installing the software on the host hard disk. After a ESXi 5.0 host is deployed with Auto Deploy, you can use Auto Deploy to upgrade, update, or apply patches to the host. To do this, you reprovision the host by rebooting it with a new image profile that contains the ESXi upgrade, update, or patch, a host configuration profile, and, optionally, third-party drivers or management agents provided by VMware partners. You can build custom images by using ESXi Image Builder CLI. See "Using vSphere Auto Deploy to Reprovision Hosts," on page 125.

esxcli

You can apply patches to ESXi 5.0 hosts using the `esxcli` command-line utility for ESXi. You cannot use `esxcli` to upgrade ESX/ESXi 4.x hosts to ESXi 5.0.x. This utility requires the vSphere CLI. See "Upgrading Hosts by Using esxcli Commands," on page 129.

The `esxupdate` and `vihostupdate` utilities are not supported for ESXi 5.0.x upgrades or updates.

Table 6-2. ESXi 5.0.x Upgrade and Update Methods

Upgrade or Update Method	Upgrade from ESX or ESXi 4.x to ESXi 5.0.x	Update or Patch from ESXi 5.0 to ESXi 5.0.x
vSphere Update Manager	yes	yes
Interactive upgrade or update from CD, DVD, or USB drive	yes	yes
Scripted upgrade or update	yes	yes
vSphere Auto Deploy	no	yes, if the ESXi 5.0 host was deployed using Auto Deploy
esxcli	no	yes

Upgrading Hosts That Have Third-Party Custom VIBs

When you upgrade a host that contains custom VIBs, the upgrade displays an error message unless the same VIBs are included in the upgrade ISO file.

A host can have custom VIBs installed, for example, for third-party drivers or management agents. For example, ESX/ESXi 4.x hosts can contain Cisco Nexus 1000V VEMs or EMC PowerPath modules. The ESXi 5.0 architecture differs from ESX/ESXi 4.x so that customized third-party software packages (VIBs) cannot be migrated when you upgrade from ESX/ESXi 4.x to ESXi 5.0. When you upgrade a 4.x host with custom VIBs that are not in the upgrade ISO, the ESXi installer displays an error message that lists the missing VIBs.

To migrate the third-party customizations as part of the host upgrade, use ESXi Image Builder to create a custom ESXi ISO image that includes the missing VIBs. For information about using Image Builder to make a custom ISO, see the information about Using ESXi Image Builder in the *vSphere Installation and Setup* documentation.

To upgrade without including the third-party software, you can take one of the following actions.

- Remove the third-party software. If you are using vSphere Update Manager, select the option to remove third-party software modules during the remediation process. For information about upgrading with vSphere Update Manager, see *Installing and Administering VMware vSphere Update Manager*.
- Override the error message during the host upgrade by selecting the Force Migrate option.

CAUTION Using either of these two options might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality. Ensure that your system does not have any critical dependence on third-party VIBs that requires resolution on first boot and cannot be resolved later. For example, your system might require custom drivers for NICs that you are booting from.

If you are upgrading a host running ESX/ESXi 4.1 Upgrade 1 or ESX/ESXi 4.0 Upgrade 3, you will see the error message for the VIBs listed in Table 6-3, even if you have never installed any custom VIBs. If you are sure that the proper functioning or your system does not depend on those VIBs, you can choose to ignore the warnings and continue with the upgrade.

Table 6-3. ESX/ESXi 4.0 U3 and 4.1 U1 Third-Party VIBs That Cannot Be Migrated to ESXi 5.0.

ESX/ESXi Release	Bulletin ID	VIB ID
4.1 Upgrade 1	ESX410-201101224-UG	cross_vmware-esx-drivers-net-vxge_400.2.0.28.21239-1OEM
4.1 Upgrade 1	ESX410-201101223-UG	cross_vmware-esx-drivers-scsi-3w-9xxx_400.2.26.08.036vm40-1OEM
4.0 Upgrade 3	ESX400-201105213-UG	cross_vmware-esx-drivers-scsi-3w-9xxx_400.2.26.08.036vm40-1OEM

Supported Upgrades and Updates to ESXi 5.0.x

You can update an ESXi 5.0 host directly to ESXi 5.0.x., and in most cases, you can migrate or upgrade an ESX 4.x or ESXi 4.x host directly to ESXi 5.0.x.

The details and level of support for an upgrade or migration from version 4.x ESX and ESXi hosts, and for an update of version 5.0 ESXi hosts, to ESXi 5.0.x depend on the host and the upgrade or update method that you use.

Table 6-4. Supported Scenarios for Upgrade or Migration to ESXi 5.0.x

Scenario for Upgrade, Migration, or Update to ESXi 5.0.x	Support
3.x ESX and ESXi hosts	Not supported for direct upgrade. You must upgrade version 3.x ESX and ESXi hosts to ESX or ESXi version 4.x before you can upgrade them to ESXi 5.0. See the vSphere 4.x upgrade documentation. Alternatively, you might find it simpler and more cost effective to do a fresh installation of ESXi 5.0.x
4.x ESX host that was upgraded from ESX 3.x with a partition layout incompatible with ESXi 5.0.x	Not supported. The VMFS partition cannot be preserved. Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200. Perform a fresh installation. To keep virtual machines, migrate them to a different system.
4.x ESX or ESXi host, migration or upgrade with vSphere Update Manager	Supported. See "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 96 and the *Installing and Administering VMware vSphere Update Manager* documentation.
4.x ESX or ESXi host, interactive migration or upgrade	Supported. See "Upgrade or Migrate Hosts Interactively," on page 110. The installer wizard offers the choice to upgrade or perform a fresh installation. If you upgrade, ESX partitions and configuration files are converted to be compatible with ESXi.
4.x ESX or ESXi host, scripted upgrade	Supported. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 111. In the upgrade script, specify the particular disk to upgrade on the system. If the system cannot be upgraded correctly because the partition table is incompatible, the installer displays a warning and does not proceed. In this case, perform a fresh installation. Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200.
4.x ESX host on a SAN or SSD	Partially supported. You can upgrade the host as you would a normal ESX 4.x host, but no provisions will be made to optimize the partitions on the disk. To optimize the partition scheme on the host, perform a fresh installation.
4.x ESX host, missing Service Console `.vmdk` file, interactive migration from CD or DVD, scripted migration, or migration with vSphere Update Manager	Not supported. The most likely reasons for a missing Service Console are that the Service Console is corrupted or that the VMFS volume is not available, which can occur if the VMFS was installed on a SAN and the LUN is not accessible. In this case, on the disk selection screen of the installer wizard, if you select a disk that has an existing ESX 4.x installation, the wizard prompts you to perform a clean installation.

Table 6-4. Supported Scenarios for Upgrade or Migration to ESXi 5.0.x (Continued)

Scenario for Upgrade, Migration, or Update to ESXi 5.0.x	Support
4.x ESX or ESXi host, asynchronously released driver or other third-party customizations, interactive migration from CD or DVD, scripted migration, or migration with vSphere Update Manager	Supported with ESXi Image Builder CLI. If a host contains customizations, such as third-party VIBS or drivers, upgrading with the standard VMware installer ISO will result in the loss of those customizations, and possibly an unstable system. Use ESXi Image Builder CLI to create a customized ESXi installer ISO file that includes the VIBs or drivers. See the information on Image Builder in the *vSphere Installation and Setup* documentation.
5.0 ESXi host	Methods supported for direct update to ESXi 5.0.x are: ■ vSphere Update Manager. Supported if you use a patch baseline, and not an upgrade baseline. ■ Interactive update from CD, DVD, or USB drive. ■ Scripted update ■ Auto Deploy (if the 5.0 ESXi host was deployed using Auto Deploy). ■ esxcli, using profile update option.

Using Manually Assigned IP Addresses for Upgrades and Migrations Performed with vSphere Update Manager

If you are using vSphere Update Manager to upgrade or migrate a host to ESXi 5.0, you must use manually assigned IP addresses for the hosts. Manually assigned IP addresses also referred to as static IP addresses.

DHCP IP addresses can cause problems during host upgrades or migrations performed with Update Manager. If a host loses its DHCP IP address during an upgrade or migration because the lease period configured on the DHCP server expires, Update Manager loses connectivity to the host. In this case, even if the host upgrade or migration is successful, Update Manager reports the upgrade or migration as failed, because it cannot connect to the host. To prevent this scenario, use manually assigned IP addresses for your hosts.

Media Options for Booting the ESXi Installer

The ESXi installer must be accessible to the system on which you are installing ESXi.

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 85.
- Boot from a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 86.
- PXE boot from the network. "PXE Booting the ESXi Installer," on page 89
- Boot from a remote location using a remote management application. See "Using Remote Management Applications," on page 96

Download and Burn the ESXi Installer ISO Image to a CD or DVD

If you do not have an ESXi installation CD/DVD, you can create one.

You can also create an installer ISO image that includes a custom installation script. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 88.

Procedure

1 Download the ISO image for ESXi from the VMware download page at http://www.vmware.com/download/.

2 Burn the ISO image to a CD or DVD.

Format a USB Flash Drive to Boot the ESXi Installation or Upgrade

You can format a USB flash drive to boot the ESXi installation or upgrade.

These instructions assume that you are performing the procedure on a Linux machine and that the USB flash drive is detected by the operating system as `/dev/sdb`.

NOTE The `ks` file containing the installation script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade.

Prerequisites

From the VMware Web site, download the ESXi ISO image `VMware-VMvisor-Installer-`*`5.x.x`*`-`*`XXXXXX`*`.x86_64.iso`, including the file `isolinux.cfg`,where *`5.x.x`* is the version of ESXi you are installing, and *`XXXXXX`* is the build number of the installer ISO image.

Procedure

1 If your USB flash drive is not detected as `/dev/sdb`, or you are not sure how your USB flash drive is detected, determine how it is detected.

   a In a terminal window, run the following command.

   ```
   tail –f /var/log/messages
   ```

   This command displays current log messages in the terminal window.

   b Plug in your USB flash drive.

   The terminal window displays several messages identifying the USB flash drive, in a format similar to the following message.

   ```
   Oct 25 13:25:23 ubuntu kernel: [  712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable
   disk
   ```

   In this example, "[sdb]" identifies the USB device. If your device is identified differently, use that identification, without the brackets, in place of sdb, in this procedure.

2 Create a partition table on the USB flash device.

   ```
   /sbin/fdisk /dev/sdb
   ```

   a Type `d` to delete partitions until they are all deleted.

   b Type `n` to create primary partition 1 that extends over the entire disk.

   c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as **c**.

   d Type `a` to set the active flag on partition 1.

   e Type `p` to print the partition table.

   The result should be similar to the following text:

   ```
   Disk /dev/sdb: 2004 MB, 2004877312 bytes
   255 heads, 63 sectors/track, 243 cylinders
   Units = cylinders of 16065 * 512 = 8225280 bytes
      Device Boot      Start         End      Blocks   Id  System
   /dev/sdb1   *           1         243     1951866    c  W95 FAT32 (LBA)
   ```

   f Type `w` to write the partition table and quit.

3 Format the USB flash drive with the Fat32 file system.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

4 Run the following commands.

```
/path_to_syslinux-3.86_directory/syslinux-3.86/bin/syslinux /dev/sdb1
cat /path_to_syslinux-3.86_directory/syslinux-3.86/usr/share/syslinux/mbr.bin > /dev/sdb
```

5 Mount the USB flash drive.

```
mount /dev/sdb1 /usbdisk
```

6 Mount the ESXi installer ISO image.

```
mount -o loop VMware-VMvisor-Installer-5.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

7 Copy the contents of the ISO image to `/usbdisk`.

```
cp -r /esxi_cdrom/* /usbdisk
```

8 Rename the `isolinux.cfg` file to `syslinux.cfg`.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

9 In the file `/usbdisk/syslinux.cfg`, change the line `APPEND -c boot.cfg` to `APPEND -c boot.cfg -p 1`.

10 Unmount the USB flash drive.

```
umount /usbdisk
```

11 Unmount the installer ISO image.

```
umount /esxi_cdrom
```

The USB flash drive can now boot the ESXi installer.

Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script

You can use a USB flash drive to store the ESXi installation script or upgrade script that is used during scripted installation or upgrade of ESXi.

When multiple USB flash drives are present on the installation machine, the installation software searches for the installation or upgrade script on all attached USB flash drives.

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

NOTE The `ks` file containing the installation or upgrade script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade.

Prerequisites

- Linux machine
- ESXi installation or upgrade script, the `ks.cfg` kickstart file
- USB flash drive

Procedure

1 Attach the USB flash drive to a Linux machine that has access to the installation or upgrade script.

2 Create a partition table.

```
/sbin/fdisk /dev/sdb
```

a Type `d` to delete partitions until they are all deleted.

b Type `n` to create primary partition 1 that extends over the entire disk.

c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as **c**.

d Type `p` to print the partition table.

The result should be similar to the following text:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *           1         243     1951866    c  W95 FAT32 (LBA)
```

e Type `w` to write the partition table and quit.

3 Format the USB flash drive with the Fat32 file system.

```
/sbin/mkfs.vfat –F 32 –n USB /dev/sdb1
```

4 Mount the USB flash drive.

```
mount /dev/sdb1 /usbdisk
```

5 Copy the ESXi installation script to the USB flash drive.

```
cp ks.cfg /usbdisk
```

6 Unmount the USB flash drive.

The USB flash drive contains the installation or upgrade script for ESXi.

What to do next

When you boot the ESXi installer, point to the location of the USB flash drive for the installation or upgrade script. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 112 and "About PXE Configuration Files," on page 92.

Create an Installer ISO Image with a Custom Installation or Upgrade Script

You can customize the standard ESXi installer ISO image with your own installation or upgrade script. This enables you to perform a scripted, unattended installation or upgrade when you boot the resulting installer ISO image.

See also "About Installation and Upgrade Scripts," on page 114 and "About the boot.cfg File," on page 122.

Prerequisites

- Linux machine.
- The ESXi ISO image `VMware-VMvisor-Installer-5.0.0-XXXXXX.x86_64.iso`, where XXXXXX is the build number of the installer ISO image.
- Your custom installation or upgrade script, the `ks_cust.cfg` kickstart file.

Procedure

1 Download the ESXi ISO image from the VMware Web site.

2 Mount the ISO image into a folder:

```
mount -o loop VMware-VMvisor-Installer-5.0.0-XXXXXX.x86_64.iso /esxi_cdrom_mount
```

XXXXXX is the ESXi build number for the version that you are installing or upgrading to.

3 Copy the contents of `cdrom` to another folder:

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

4 Copy the kickstart file to `/esxi_cdrom`

```
cp ks_custom.cfg /esxi_cdrom
```

5 (Optional) Modify the `boot.cfg` file to specify the location of the installation or upgrade script using the `kernelopt` option.

This step makes the installation or upgrade completely automatic, without the need to specify the kickstart file during the installation or upgrade.

6 Recreate the ISO image:

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot
-boot-load-size 4 -boot-info-table /esxi_cdrom
```

The ISO image now includes your custom installation or upgrade script.

What to do next

Install ESXi from the ISO image.

PXE Booting the ESXi Installer

You use the preboot execution environment (PXE) to boot a host and launch the ESXi installer from a network interface.

ESXi 5.0 is distributed in an ISO format that is designed to install to flash memory or to a local hard drive. You can extract the files and boot using PXE.

PXE uses DHCP and Trivial File Transfer Protocol (TFTP) to boot an operating system over a network.

PXE booting requires some network infrastructure and a machine with a PXE-capable network adapter. Most machines that are capable of running ESXi have network adapters that are able to PXE boot.

NOTE Ensure that the Auto Deploy server has an IPv4 address. PXE booting is supported only with IPv4.

About the TFTP Server, PXELINUX, and gPXE

Trivial File Transfer Protocol (TFTP) is similar to the FTP service, and is typically used only for network booting systems or loading firmware on network devices such as routers.

Most Linux distributions include a copy of the tftp-hpa server. If you require a supported solution, purchase a supported TFTP server from your vendor of choice.

If your TFTP server will run on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/. Earlier versions of tftpd32 were incompatible with PXELINUX and gPXE.

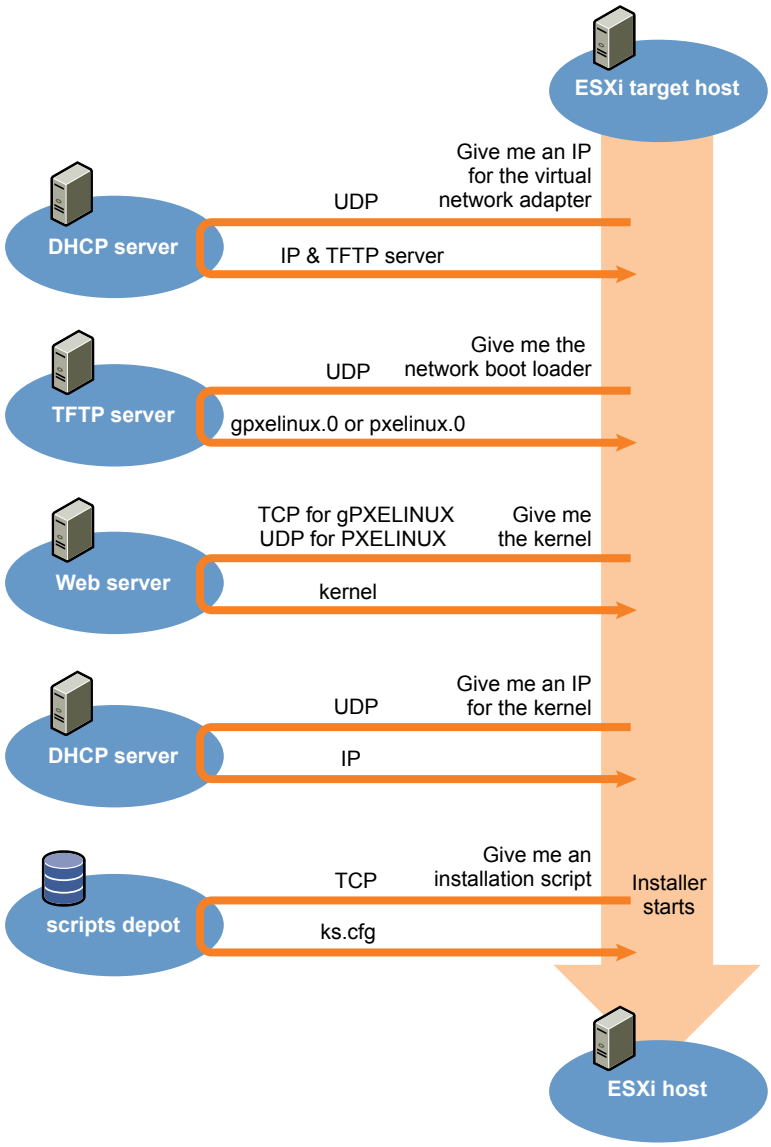
You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.

The PXELINUX and gPXE environments allow your target machine to boot the ESXi installer. PXELINUX is part of the SYSLINUX package, which can be found at http://www.kernel.org/pub/linux/utils/boot/syslinux/, although many Linux distributions include it. Many versions of PXELINUX also include gPXE. Some distributions, such as Red Hat Enterprise Linux version 5.3, include earlier versions of PXELINUX that do not include gPXE.

If you do not use gPXE, you might experience problems while booting the ESXi installer on a heavily loaded network TFTP is sometimes unreliable for transferring large amounts of data. If you use PXELINUX without gPXE, the `pxelinux.0` binary file, the configuration file, the kernel, and other files are transferred by TFTP. If you use gPXE, only the `gpxelinux.0` binary file and configuration file are transferred by TFTP. With gPXE, you can use a Web server to transfer the kernel and other files required to boot the ESXi installer.

NOTE VMware tests PXE booting with PXELINUX version 3.86. This is not a statement of limited support. For support of third-party agents that you use to set up your PXE booting infrastructure, contact the vendor.

Figure 6-1. Overview of PXE Boot Installation Process



Sample DHCP Configuration

To PXE boot the ESXi installer, the DHCP server must send the address of the TFTP server and a pointer to the `pxelinux.0` or `gpxelinux.0` directory.

The DHCP server is used by the target machine to obtain an IP address. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the PXELINUX binary (which usually resides on a TFTP server). When the target machine first boots, it broadcasts a packet across the network requesting this information to boot itself. The DHCP server responds.

Caution Do not set up a new DHCP server if your network already has one. If multiple DHCP servers respond to DHCP requests, machines can obtain incorrect or conflicting IP addresses, or can fail to receive the proper boot information. Talk to a network administrator before setting up a DHCP server. For support on configuring DHCP, contact your DHCP server vendor.

Many DHCP servers can PXE boot hosts. If you are using a version of DHCP for Microsoft Windows, see the DHCP server documentation to determine how to pass the `next-server` and `filename` arguments to the target machine.

gPXE Example

This example shows how to configure a ISC DHCP version 3.0 server to enable gPXE.

```
allow booting;
allow bootp;
# gPXE options
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.bus-id code 177 = string
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server TFTP server address;
   if not exists gpxe.bus-id {
      filename "/gpxelinux.0";
   }
}
subnet Network address netmask Subnet Mask {
   range Starting IP Address Ending IP Address;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `gpxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

PXELINUX (without gPXE) Example

This example shows how to configure a ISC DHCP version 3.0 server to enable PXELINUX.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xx.xx;
```

```
   filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
   range 192.168.48.100 192.168.48.250;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

About PXE Configuration Files

The PXE configuration file defines the menu displayed to the target ESXi host as it boots up and contacts the TFTP server. You need a PXE configuration file to PXE boot the ESXi installer.

The TFTP server constantly listens for PXE clients on the network. When it detects that a PXE client is requesting PXE services, it sends the client a network package that contains a boot menu.

Required Files

In the PXE configuration file, you must include paths to the following files:

- `mboot.c32` is the boot loader.
- `boot.cfg` is the boot loader configuration file.

See "About the boot.cfg File," on page 122

File Name for the PXE Configuration File

For the file name of the PXE configuration file, select one of the following options:

- `01-`*`mac_address_of_target_ESXi_host`*. For example, `01-23-45-67-89-0a-bc`
- The target ESXi host IP address in hexadecimal notation.
- `default`

The initial boot file, `pxelinux.0` or `gpxelinux.0`, tries to load a PXE configuration file. It tries with the MAC address of the target ESXi host, prefixed with its ARP type code, which is 01 for Ethernet. If that attempt fails, it tries with the hexadecimal notation of target ESXi system IP address. Ultimately, it tries to load a file named `default`.

File Location for the PXE Configuration File

Save the file in `var/lib/tftpboot/pxelinux.cfg/` on the TFTP server.

For example, you might save the file on the TFTP server at `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. The MAC address of the network adapter on the target ESXi host is 00-21-5a-ce-40-f6.

PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File

You can use a TFTP server to PXE boot the ESXi installer, using PXELINUX and a PXE configuration file.

See also "About Installation and Upgrade Scripts," on page 114 and "About the boot.cfg File," on page 122

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site.
- TFTP server that supports PXE booting with gPXE. See "About the TFTP Server, PXELINUX, and gPXE," on page 89.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 91.

- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.0. See the Hardware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See "About Installation and Upgrade Scripts," on page 114.
- Network adapter with PXE support on the target ESXi host
- IPv4 networking. IPv6 is not supported for PXE booting.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Create the `/tftpboot/pxelinux.cfg` directory on your TFTP server.

2 On the Linux machine, install PXELINUX.

PXELINUX is included in the SYSLINUX package. Extract the files, locate the `pxelinux.0` file and copy it to the `/tftpboot` directory on your TFTP server.

3 Configure the DHCP server to send the following information to each client host:

- The name or IP address of your TFTP server.
- The name of your initial boot file. This is `pxelinux.0`.

4 Copy the contents of the ESXi installer image to the `/var/lib/tftpboot` directory on the TFTP server.

5 (Optional) For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option on the line following the kernel command, to specify the location of the installation script.

Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory containing the `ks.cfg` file.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

6 Create a PXE configuration file.

This file defines how the host boots when no operating system is present. The PXE configuration file references the boot files. Use the following code as a model, where `XXXXXX` is the build number of the ESXi installer image.

```
DEFAULT menu.c32
MENU TITLE ESXi-5.0.0-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-5.0.0-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Name the file with the MAC address of the target host machine: `01-`*`mac_address_of_target_ESXi_host`*.

For example, `01-23-45-67-89-0a-bc`.

8 Save the PXE configuration file in `/tftpboot/pxelinux.cfg` on the TFTP server.

9 Boot the machine with the network adapter.

PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File

You can PXE boot the ESXi installer using PXELINUX, and use the isolinux.cfg file as the PXE configuration file.

See also "About Installation and Upgrade Scripts," on page 114 and "About the boot.cfg File," on page 122

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site.
- TFTP server that supports PXE booting with PXELINUX. See "About the TFTP Server, PXELINUX, and gPXE," on page 89.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 91.
- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.0. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See "About Installation and Upgrade Scripts," on page 114.
- Network adapter with PXE support on the target ESXi host
- IPv4 networking. IPv6 is not supported for PXE booting.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Create the `/tftpboot/pxelinux.cfg` directory on your TFTP server.

2 On the Linux machine, install PXELINUX.

  PXELINUX is included in the SYSLINUX package. Extract the files, locate the file `pxelinux.0` and copy it to the `/tftpboot` directory on your TFTP server.

3 Configure the DHCP server.

  The DHCP server sends the following information to your client hosts:

  - The name or IP address of your TFTP server.
  - The name of your initial boot file. This is `pxelinux.0`.

4 Copy the contents of the ESXi installer image to the `/var/lib/tftpboot` directory on the TFTP server.

5 (Optional) For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option on the next line after the `kernel` command, to specify the location fo the installation script.

  In the following example, *XXX.XXX.XXX.XXX* is the IP address of the server where the installation script resides.

  `kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg`

6 Copy the `isolinux.cfg` file from the ESXi installer ISO image to the `/tftpboot/pxelinux.cfg` directory.

The `isolinux.cfg` file contains the following code, where `XXXXXX` is the build number of the ESXi installer image:

```
DEFAULT menu.c32
MENU TITLE ESXi-5.0.0-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-5.0.0-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Rename the `isolinux.cfg` file with the MAC address of the target host machine: `01-`*`mac_address_of_target_ESXi_host`*. For example, `01-23-45-67-89-0a-bc`

8 Boot the machine with the network adapter.

PXE Boot the ESXi Installer Using gPXE

You can PXE boot the ESXi installer using gPXE.

See also "About Installation and Upgrade Scripts," on page 114 and "About the boot.cfg File," on page 122

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site
- HTTP Web server that is accessible by your target ESXi hosts
- DHCP server configured for PXE booting: `/etc/dhcpd.conf` is configured for client hosts with a TFTP server and the initial boot file set to `gpxelinux.0/undionly.kpxe`. See "Sample DHCP Configuration," on page 91.
- Server with a hardware configuration that is supported with ESXi 5.0. See the Hardware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.
- gPXELINUX
- (Optional) ESXi installation script. See "About Installation and Upgrade Scripts," on page 114.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Copy the contents of the ESXi installer ISO image to the `/var/www/html` directory on the HTTP server.

2 Modify the `boot.cfg` file with the information for the HTTP server.

Use the following code as a model, where *XXX.XXX.XXX.XXX* is the HTTP server IP address. The `kernelopt` line is optional. Include that option to specify the location of the installation script for a scripted installation.

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz ---
```

```
http://XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 ---
http://XXX.XXX.XXX.XXX/s.v00 --- http://XXX.XXX.XXX.XXX/weaselin.v00 ---
http://XXX.XXX.XXX.XXX/tools.t00 --- http://XXX.XXX.XXX.XXX/imgdb.tgz ---
http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

3 gPXE boot the host and press Ctrl+B to access the GPT menu.

4 Enter the following commands to boot with the ESXi installer, where *XXX.XXX.XXX.XXX* is the HTTP server IP address.

```
dhcp net0 ( if dchp is not set)
kernel –n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 –c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

Using Remote Management Applications

Remote management applications allow you to install ESXi on servers that are in remote locations.

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see "Supported Remote Management Server Models and Minimum Firmware Versions," on page 25. For support on remote management applications, contact the vendor.

You can use remote management applications to do both interactive and scripted installations of ESXi remotely.

If you use remote management applications to install ESXi, the virtual CD might encounter corruption problems with systems or networks operating at peak capacity. If a remote installation from an ISO image fails, complete the installation from the physical CD media.

Performing the Upgrade or Migration

Several tools are available to upgrade and migrate hosts. You can use different upgrade tools based depending on the type of host you are upgrading (ESX or ESXi) and whether the hosts are managed by vCenter Server.

You can migrate or upgrade from version 4.x ESX or ESXi to ESXi 5.0 with the tools and methods described in "ESXi 5.0.x Upgrade and Update Options," on page 82.

To upgrade version 3.5 ESX or ESXi to ESXi 5.0, you must first upgrade version 3.5 ESX or ESXi to version 4.x ESX or ESXi. See the VMware vSphere 4.x documentation Web page for information about upgrading from version 3.5 ESX or ESXi 3.5 to version 4.x ESX or ESXi.

Caution If you upgrade hosts managed by vCenter Server, you must upgrade to vCenter Server before you upgrade ESX or ESXi. If you do not upgrade in the correct order, you can lose data and lose access to your servers.

Using vSphere Update Manager to Perform Orchestrated Host Upgrades

Orchestrated upgrades allow you to upgrade the objects in your vSphere inventory in a two-step process: host upgrades, followed by virtual machine upgrades. You can configure the process at the cluster level to automate more of the process, or you can configure it at the individual host or virtual machine level for granular control.

For example, you can define a host upgrade baseline to upgrade an ESXi 4.x host to ESXi 5.0, or you can define a virtual machine upgrade baseline to upgrade the VMware Tools and the virtual machine hardware to the latest version. Use wizard-based workflows to first schedule host upgrades for an entire cluster and then schedule a virtual machine upgrade for all the virtual machines.

You cannot use Update Manager to upgrade a host to ESXi 5.0 if the host was previously upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. This problem also affects some 4.x ESX hosts, even if they were not previously upgraded from ESX 3.x. Hosts must have more than 350MB of free space in the /boot partition to support the Update Manager upgrade process. If the host that you are upgrading does not have more than 350MB of free space in the /boot partition, use a scripted or interactive upgrade instead.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

The wizard workflows prevent erroneous upgrade sequences. For example, the wizard prevents you from upgrading virtual machine hardware before you upgrade hosts in a cluster.

You can use Distributed Resource Scheduler (DRS) to prevent virtual machine downtime during the upgrade process.

Update Manager monitors hosts and virtual machines for compliance against your defined upgrade baselines. Noncompliance appears in detailed reports and in the dashboard view. Update Manager supports mass remediation.

The following vSphere components are upgraded by Update Manager.

- ESX and ESXi kernel (vmkernel)
- Virtual machine hardware
- VMware Tools
- Virtual appliances

For components that are not listed here, you can perform the upgrade by using another upgrade method, or, for third-party components, by using the appropriate third-party tools.

The following topics describe how to use Update Manager to conduct an orchestrated upgrade of your ESXi hosts.

- "Configuring Host and Cluster Settings," on page 97
- "Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager," on page 98

To use Update Manager to conduct an orchestrated upgrade of virtual machines on your hosts, see "Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager," on page 147. For complete documentation of all Update Manager operations, see the *vSphere Update Manager Installation and Administration Guide*.

Configuring Host and Cluster Settings

When you update vSphere objects in a cluster with DRS, VMware High Availability (HA), and VMware Fault Tolerance (FT) enabled, you can choose to temporarily disable VMware Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update completes, Update Manager restores these features.

Updates might require that the host enters maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, vCenter Server can migrate virtual machines to other ESX/ESXi hosts within a cluster before the host is put into maintenance mode. vCenter Server migrates the virtual machines if the cluster is configured for vMotion, and if DRS is enabled.

If a host has no running virtual machines, VMware DPM might put the host in standby mode and interrupt an Update Manager operation. To make sure that scanning and staging complete successfully, Update Manager disables VMware DPM during these operations. To ensure successful remediation, you should allow Update Manager to disable VMware DPM and HA admission control before the remediation operation. After the operation completes, Update Manager restores VMware DPM and HA admission control. Update Manager disables HA admission control before staging and remediation but not before scanning.

If VMware DPM has already put hosts in standby mode, Update Manager powers on the hosts before scanning, staging, and remediation. After the scanning, staging, or remediation is complete, Update Manager turns on VMware DPM and HA admission control and lets VMware DPM put hosts into standby mode, if needed. Update Manager does not remediate powered off hosts.

If hosts are put into standby mode and VMware DPM is manually disabled for a reason, Update Manager does not remediate or power on the hosts.

Within a cluster, you should select to temporarily disable HA admission control to allow vMotion to proceed, in order to prevent downtime of the machines on the hosts you remediate. After the remediation of the entire cluster, Update Manager restores HA admission control settings.

If FT is turned on for any of the virtual machines on hosts within a cluster, you should select to temporarily turn off FT before performing any Update Manager operations on the cluster. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. You should remediate all hosts in a cluster with the same updates, so that FT can be re-enabled after the remediation, because a primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESX/ESXi version and patch level.

Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager

You can use Update Manager to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory by using a single upgrade baseline, or by using a baseline group.

This workflow describes the overall process to perform an orchestrated upgrade of the hosts in your vSphere inventory. Update Manager 5.0 supports host upgrades to ESXi 5.0 for hosts that are running ESX/ESXi 4.x.

You can perform orchestrated upgrades of hosts at the folder, cluster, or datacenter level.

NOTE The last two steps in this procedure are alternatives. Choose one or the other.

Prerequisites

- Make sure your system meets the requirements for vCenter Server 5.0, ESXi 5.0, and Update Manager 5.0. See "Update Manager Hardware Requirements," on page 25
- Install or upgrade vCenter Server to version 5.0. See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.
- Install or upgrade vSphere Update Manager to version 5.0. See Chapter 5, "Upgrading Update Manager," on page 71.

Procedure

1 Configure Host Maintenance Mode Settings on page 99

ESX/ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESX/ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

2 Configure Cluster Settings on page 100

For ESX/ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

3 Enable Remediation of PXE Booted ESXi 5.0 Hosts on page 101

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi 5.x hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

4 Import Host Upgrade Images and Create Host Upgrade Baselines on page 102

You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.x images that you import to the Update Manager repository.

5 Create a Host Baseline Group on page 103

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

6 Attach Baselines and Baseline Groups to Objects on page 104

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.

7 Manually Initiate a Scan of ESX/ESXi Hosts on page 104

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

8 View Compliance Information for vSphere Objects on page 105

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

9 Remediate Hosts Against an Upgrade Baseline on page 105

You can remediate ESX/ESXi hosts against a single attached upgrade baseline at a time. You can upgrade or migrate all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 5.0 image.

10 Remediate Hosts Against Baseline Groups on page 108

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

Configure Host Maintenance Mode Settings

ESX/ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESX/ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

For hosts in a container different from a cluster or for individual hosts, migration of the virtual machines with vMotion cannot be performed. If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

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 **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Under Maintenance Mode Settings, select an option from the **VM Power state** drop-down menu to determine the change of the power state of the virtual machines and appliances that are running on the host to be remediated.

Option	Description
Power Off virtual machines	Powers off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspends all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leaves virtual machines and virtual appliances in their current power state. This is the default setting.

3 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the retry delay, and the number of retries.

If a host fails to enter maintenance mode before remediation, Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

4 (Optional) Select **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode**.

Update Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation.

After remediation, Update Manager reconnects the removable media devices if they are still available.

5 Click **Apply**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Configure Cluster Settings

For ESX/ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

NOTE Remediating hosts in parallel can improve performance significantly by reducing the time required for cluster remediation. Update Manager remediates hosts in parallel without disrupting the cluster resource constraints set by DRS.

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 **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Select the check boxes for features that you want to disable or enable.

Option	Description
Distributed Power Management (DPM)	VMware DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. If you do not choose to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you choose to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates the hosts in the cluster, and re-enables VMware DPM after remediation is complete.
High Availability (HA) admission control	Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. If you do not choose to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you choose to temporarily disable HA admission control, Update Manager disables HA admission control, remediates the cluster, and re-enables HA admission control after remediation is complete.
Fault Tolerance (FT)	FT provides continuous availability for virtual machines by automatically creating and maintaining a secondary virtual machine that is identical to the primary virtual machine. If you do not choose to turn off FT for the virtual machines on a host, Update Manager does not remediate that host.
Enable parallel remediation for hosts in cluster	Update Manager can remediate hosts in clusters in a parallel manner. Update Manager continuously evaluates the maximum number of hosts it can remediate in parallel without disrupting DRS settings. If you do not select the option, Update Manager remediates the hosts in a cluster sequentially.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can select to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

3 Click **Apply**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Enable Remediation of PXE Booted ESXi 5.0 Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi 5.x hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

The global setting in the Update Manager **Configuration** tab enables solutions such as ESX Agent Manager or Cisco Nexus 1000V to initiate remediation of PXE booted ESXi 5.x hosts. In contrast, the **Enable patch remediation of powered on PXE booted ESXi hosts** setting in the Remediate wizard enables Update Manager to patch PXE booted hosts.

To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with Update Manager, so that the updates are not lost because of a reboot. For more information about creating custom ESXi images, see *Image Builder Administration*. Update Manager itself does not reboot the hosts because it does not install updates requiring a reboot on PXE booted ESXi 5.0 hosts.

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 **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 To enable installation of software for solutions on PXE booted ESXi.5x hosts, select **Allow installation of additional software on PXE booted ESXi 5.x hosts.**

3 Click **Apply**.

Import Host Upgrade Images and Create Host Upgrade Baselines

You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.x images that you import to the Update Manager repository.

You can use ESXi `.iso` images to upgrade ESXi 4.x hosts to ESXi 5.x or migrate ESX 4.x hosts to ESXi 5.x.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using Image Builder.

Prerequisites

Ensure that you have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

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 **ESXi Images** tab click **Import ESXi Image** on the upper-right side.

2 On the Select ESXi Image page of the Import ESXi Image wizard, browse to and select the ESXi image that you want to upload.

3 Click **Next**.

CAUTION Do not close the import wizard. Closing the import wizard stops the upload process.

4 (Optional) In the Security Warning window, select an option to handle the certificate warning.

A trusted certificate authority does not sign the certificates that are generated for vCenter Server and ESX/ESXi hosts during installation. Because of this, each time an SSL connection is made to one of these systems, the client displays a warning.

Option	Action
Ignore	Click **Ignore** to continue using the current SSL certificate and start the upload process.
Cancel	Click **Cancel** to close the window and stop the upload process.
Install this certificate and do not display any security warnings	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

5 After the file is uploaded, click **Next**.

6 (Optional) Create a host upgrade baseline.

   a Leave the **Create a baseline using the ESXi image** selected.

   b Specify a name, and optionally, a description for the host upgrade baseline.

7 Click **Finish**.

The ESXi image that you uploaded appears in the Imported ESXi Images pane. You can see more information about the software packages that are included in the ESXi image in the Software Packages pane.

If you also created a host upgrade baseline, the new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

What to do next

To upgrade or migrate the hosts in your environment, you must create a host upgrade baseline if you have not already done so.

Create a Host Baseline Group

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a 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 Enter a unique name for the baseline group.

3 Under Baseline Group Type, select **Host Baseline Group** and click **Next**.

4 Select a host upgrade baseline to include it in the baseline group.

5 (Optional) Create a new host upgrade baseline by clicking **Create a new Host Upgrade Baseline** at the bottom of the Upgrades page and complete the New Baseline wizard.

6 Click **Next**.

7 Select the patch baselines that you want to include in the baseline group.

8 (Optional) Create a new patch baseline by clicking **Create a new Host Patch Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

9 Click **Next**.

10 Select the extension baselines to include in the baseline group.

11 (Optional) Create a new extension baseline by clicking **Create a new Extension Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

12 On the Ready to Complete page, click **Finish**.

The host 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.

Manually Initiate a Scan of ESX/ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.

2 Right-click a host, datacenter, or any container object and select **Scan for Updates**.

3 Select the types of updates to scan for.

You can scan for either **Patches and Extensions** or **Upgrades**.

4 Click **Scan**.

The selected inventory object and all child objects are scanned against all patches, extensions, and upgrades in the attached baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

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.

Remediate Hosts Against an Upgrade Baseline

You can remediate ESX/ESXi hosts against a single attached upgrade baseline at a time. You can upgrade or migrate all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 5.0 image.

NOTE Alternatively, you can upgrade hosts by using a baseline group. See "Remediate Hosts Against Baseline Groups," on page 108.

Update Manager 5.0 supports only upgrade from ESXi 4.x to ESXi 5.x and migration from ESX 4.x to ESXi 5.x. You cannot use Update Manager to upgrade a host to ESXi 5.0 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the `/boot` partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using Image Builder.

NOTE In case of an unsuccessful upgrade or migration from ESX/ESXi 4.x to ESXi 5.x, you cannot roll back to your previous ESX/ESXi 4.x instance.

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.

To remediate a host against an upgrade baseline, attach the baseline to the host.

Review any scan messages in the Upgrade Details window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade or migration to ESXi 5.0.

Procedure

1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

If you select a container object, all hosts under the selected object are remediated.

3 On the Remediation Selection page of the Remediate wizard, select the upgrade baseline to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESXi 5.x Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.x your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

7 Click **Next**.

8 On the Schedule page, specify a unique name and an optional description for the task.

9 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

10 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

11 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

12 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

13 Click **Next**.

14 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. NOTE Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

16 On the Ready to Complete page, click **Finish**.

Remediate Hosts Against Baseline Groups

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

You can perform an orchestrated upgrade by using a host baseline group. The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

Note Alternatively, you can upgrade hosts by using a single upgrade baseline. See "Remediate Hosts Against an Upgrade Baseline," on page 105.

Prerequisites

Ensure that at least one baseline group is attached to the host.

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.

Review any scan messages in the Upgrade Details window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade or migration to ESXi 5.0.

Procedure

1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

If you select a container object, all hosts under the selected object are remediated.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and baselines to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESXi 5.x Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.x your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

7 Click **Next**.

8 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process, and click **Next**.

9 (Optional) On the Dynamic Patches and Extensions to Exclude page, review the list of patches or extensions to be excluded and click **Next**.

10 On the Schedule page, specify a unique name and an optional description for the task.

11 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

12 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

13 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

14 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

15 (Optional) Select the check box under ESXi 5.x Patch Settings to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

16 Click **Next**.

17 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.

Option	Details
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. NOTE Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

18 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

19 On the Ready to Complete page, click **Finish**.

Upgrade or Migrate Hosts Interactively

You can boot the ESXi installer from a CD, DVD, or USB flash drive to upgrade ESX/ESXi 4.x hosts to ESXi 5.0.

IMPORTANT If you are performing a fresh ESXi installation, see the *vSphere Installation and Setup* documentation. The instructions in this *vSphere Upgrade* documentation are for an upgrade or migration of ESXi or ESX.

Before upgrading, consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. 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.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Prerequisites

- You must have the ESXi installer ISO in one of the following locations.
  - On CD or DVD. If you do not have the installation CD/DVD, you can create one. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 85
  - On a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 86

  NOTE You can also PXE boot the ESXi installer to launch an interactive installation or a scripted installation. See "PXE Booting the ESXi Installer," on page 89.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- ESXi Embedded must not be on the host. ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1 Insert the ESXi installer CD/DVD into the CD/DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.

2 Set the BIOS to boot from the CD-ROM device or the USB flash drive.

See your hardware vendor documentation for information on changing boot order.

3 In the Select a Disk panel, 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. On systems where drives are continuously being added and removed, they might be out of order.

4 If the installer finds an existing ESX or ESXi installation and VMFS datastore you can choose from the following options:

- **Upgrade ESXi, preserve VMFS datastore**
- **Install ESXi, preserve VMFS datastore**
- **Install ESXi, overwrite VMFS datastore**

If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

If the existing ESX or ESXi installation contains custom VIBs that are not included in the ESXi installer ISO, the option **Upgrade ESXi, preserve VMFS datastore** is replaced with **Force Migrate ESXi, preserve VMFS datastore**.

CAUTION Using the Force Migrate option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality. See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 83.

5 Press F11 to confirm and start the upgrade.

6 When the upgrade is complete, remove the installation CD/DVD or USB flash drive.

7 Press Enter to reboot the host.

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

If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

See your hardware vendor documentation for information on changing boot order.

Installing, Upgrading, or Migrating Hosts Using a Script

You can quickly deploy ESXi hosts using scripted, unattended installations or upgrades. Scripted installations, upgrades, or migrations provide an efficient way to deploy multiple hosts.

The installation or upgrade script contains the installation settings for ESXi. You can apply the script to all hosts that you want to have a similar configuration.

For a scripted installation, upgrade, or migration, you must use the supported commands to create a script. and edit the script to change settings that are unique for each host.

The installation or upgrade script can reside in one of the following locations:

- FTP

- HTTP/HTTPS
- NFS
- USB flash drive
- CDROM

Enter Boot Options to Start an Installation or Upgrade Script

You can start an installation or upgrade script by typing boot command-line options at the boot command line.

At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See "About the boot.cfg File," on page 122 and "PXE Booting the ESXi Installer," on page 89.

A `ks=...` option must be given, to specify the location of the installation script. Otherwise, a scripted installation or upgrade will not start. If `ks=...` is omitted, the text installer will proceed.

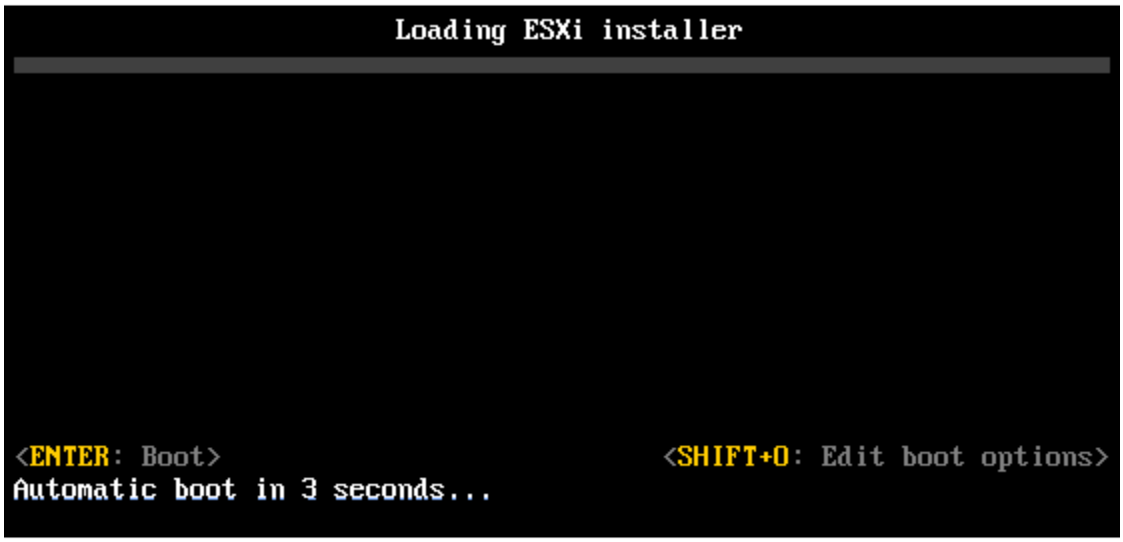
Supported boot options are listed in "Boot Options," on page 113.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Procedure

1 Start the host.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 At the `runweasel` command prompt, type
`ks=`*`location of installation script plus boot command line options`*

Example: Boot Option

You type the following boot options:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Boot Options

When you perform a scripted installation, you might need to specify options at boot time to access the kickstart file.

Supported Boot Options

Table 6-5. Boot Options for ESXi Installation

Boot Option	Description
`BOOTIF=`*`hwtype-MAC address`*	Similar to the `netdevice` option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`gateway=`*`ip address`*	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
`ip=`*`ip address`*	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`ks=cdrom:/`*`path`*	Performs a scripted installation with the script at *path*, which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found.
`ks=file://`*`path`*	Performs a scripted installation with the script at *path*.
`ks=`*`protocol`*`://`*`serverpath`*	Performs a scripted installation with a script located on the network at the given URL. *protocol* can be `http`, `https`, `ftp`, or `nfs`. The format of an NFS URL is specified in RFC 2224.
`ks=usb`	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named `ks.cfg`. The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the `ks.cfg` file is found. Only FAT16 and FAT32 file systems are supported.
`ks=usb:/`*`path`*	Performs a scripted installation with the script file at the specified path, which resides on USB.
`ksdevice=`*`device`*	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`nameserver=`*`ip address`*	Specifies a domain name server to be used for downloading the installation script and installation media.
`netdevice=`*`device`*	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`netmask=`*`subnet mask`*	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
`vlanid=`*`vlanid`*	Configure the network card to be on the specified VLAN.

About Installation and Upgrade Scripts

The installation/upgrade script is a text file, for example `ks.cfg`, that contains supported commands.

The command section of the script contains the ESXi installation options. This section is required and must appear first in the script.

Locations Supported for Installation or Upgrade Scripts

In scripted installations and upgrades, the ESXi installer can access the installation or upgrade script, also called the kickstart file, from several locations.

The following locations are supported for the installation or upgrade script:

- CD/DVD. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 88.
- USB Flash drive. See "Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script," on page 87.
- A location accessible with the following protocols: NFS, HTTP, HTTPS, FTP

Path to the Installation or Upgrade Script

You can specify the path to an installation or upgrade script.

`ks=http://`*`XXX.XXX.XXX.XXX`*`/kickstart/KS.CFG` is the path to the ESXi installation script, where *`XXX.XXX.XXX.XXX`* is the IP address of the machine where the script resides. See "About Installation and Upgrade Scripts," on page 114.

To start an installation script from an interactive installation, you enter the `ks=` option manually. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 112.

Installation and Upgrade Script Commands

To modify the default installation or upgrade script or to create your own script, use supported commands. Use supported commands in the installation script, which you specify with a boot command when you boot the installer.

To determine which disk to install or upgrade ESXi on, the installation script requires one of the following commands: `install`, `upgrade`, or `installorupgrade`. The `install` command creates the default partitions, including a VMFS datastore that occupies all available space after the other partitions are created. The `install` command replaces the `autopart` command that was used for scripted ESXi 4.1 installations.

accepteula or vmaccepteula (required)

Accepts the ESXi license agreement. This command functions as it did in ESXi 4.1.

clearpart (optional)

Compared to kickstart, the behavior of the ESXi `clearpart` command is different. Carefully edit the `clearpart` command in your existing scripts.

Clears any existing partitions on the disk. Requires `install` command to be specified.

`--drives=`	Remove partitions on the specified drives.
`--alldrives`	Ignores the `--drives=` requirement and allows clearing of partitions on every drive.
`--ignoredrives=`	Removes partitions on all drives except those specified. Required unless the `--drives=` or `--alldrives` flag is specified.

--overwritevmfs

Permits overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.

--firstdisk=
disk-type1
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

dryrun (optional)

Parses and checks the installation script. Does not perform the installation.

install

Specifies that this is a fresh installation. Replaces the deprecated `autopart` command used for ESXi 4.1 scripted installations. Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*diskname*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 121.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

--overwritevmfs Required to overwrite an existing VMFS datastore on the disk before installation.

--preservevmfs Preserves an existing VMFS datastore on the disk during installation.

--novmfsondisk Prevents a VMFS partition from being created on this disk. Must be used with --overwritevmfs if a VMFS partition already exists on the disk.

installorupgrade

Either the install, upgrade, or installorupgrade command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive= Specifies the disk to partition. In the command --disk=*diskname*, the *diskname* can be in any of the forms shown in the following examples:

- Path: --disk=*/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0*
- MPX name: --disk=*mpx.vmhba1:C0:T0:L0*
- VML name: --disk=*vml.000000034211234*
- vmkLUN UID: --disk=*vmkLUN_UID*

For accepted disk name formats, see "Disk Device Names," on page 121.

--firstdisk=
disk-type1,
[*disk-type2*,...] Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (local)

2 Network storage (remote)

3 USB disks (usb)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local.

--overwritevmfs Install ESXi if a VMFS partition exists on the disk, but no ESX or ESXi installation exists. Unless this option is present, the installer will fail if a VMFS partition exists on the disk, but no ESX or ESXi installation exists.

--forcemigrate If the host contains customizations, such as third-party VIBS or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The forcemigrate option overrides the error and forces the upgrade.

CAUTION Using the forcemigrate option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.

keyboard (optional)

Sets the keyboard type for the system.

keyboardType Specifies the keyboard map for the selected keyboard type. *keyboardType* must be one of the following types.

- Belgian
- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Default
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- US Dvorak
- Ukranian
- United Kingdom

network (optional)

Specify a network address for the system.

--bootproto=[dhcp|static]	Specify whether to obtain the network settings from DHCP or set them manually.
--device=	Specifies either the MAC address of the network card or the device name, in the form `vmnicNN`, as in `vmnic0`. This options refers to the uplink device for the virtual switch.
--ip=	Sets an IP address for the machine to be installed, in the form `xxx.xxx.xxx.xxx`. Required with the `--bootproto=static` option and ignored otherwise.
--gateway=	Designates the default gateway as an IP address, in the form `xxx.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--nameserver=	Designates the primary name server as an IP address. Used with the `--bootproto=static` option. Omit this option if you do not intend to use DNS. The `--nameserver` option can accept two IP addresses. For example: `--nameserver="10.126.87.104[,10.126.87.120]"`
--netmask=	Specifies the subnet mask for the installed system, in the form `255.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--hostname=	Specifies the host name for the installed system.
--vlanid= ***vlanid***	Specifies which VLAN the system is on. Used with either the `--bootproto=dhcp` or `--bootproto=static` option. Set to an integer from 1 to 4096.
--addvmportgroup=(0|1)	Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (optional)

Causes warning messages to interrupt the installation. If you omit this command, warning messages are logged.

part or partition (optional)

Creates an additional VMFS datastore on the system. Only one datastore per disk can be created. Cannot be used on the same disk as the `install` command. Only one partition can be specified per disk and it can only be a VMFS partition

datastore name	Specifies where the partition is to be mounted
--ondisk= or --ondrive=	Specifies the disk or drive where the partition is created.
--firstdisk= ***disk-type1,*** **[*disk-type2*,...]**	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: 1 Locally attached storage (`local`) 2 Network storage (`remote`) 3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

reboot (optional)

Reboots the machine after the scripted installation is complete.

`<--noeject>` The CD is not ejected after the installation.

rootpw (required)

Sets the root password for the system.

`--iscrypted` Specifies that the password is encrypted.

password Specifies the password value.

upgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

`--disk= or --drive=` Specifies the disk to partition. In the command `--disk=`*diskname*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0*
- MPX name: `--disk=`*mpx.vmhba1:C0:T0:L0*
- VML name: `--disk=`*vml.000000034211234*
- vmkLUN UID:`--disk=`*vmkLUN_UID*

For accepted disk name formats, see "Disk Device Names," on page 121.

`--firstdisk=`
disk-type1,
`[`*`disk-type2`*`,...]`

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

--deletecosvmdk — If the system is being upgraded from ESX, remove the directory that contains the old Service Console VMDK file, `cos.vmdk`, to reclaim unused space in the VMFS datastore.

--forcemigrate — If the host contains customizations, such as third-party VIBS or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The `forcemigrate` option overrides the error and forces the upgrade.

CAUTION Using the `forcemigrate` option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.

%include or include (optional)

Specifies another installation script to parse. This command is treated similarly to a multiline command, but takes only one argument.

filename — For example: `%include part.cfg`

%pre (optional)

Specifies a script to run before the kickstart configuration is evaluated. For example, you can use it to generate files for the kickstart file to include.

--interpreter =[python|busybox] — Specifies an interpreter to use. The default is busybox.

%post (optional)

Runs the specified script after package installation is complete. If you specify multiple `%post` sections, they run in the order that they appear in the installation script.

--interpreter =[python|busybox] — Specifies an interpreter to use. The default is busybox.

--timeout=secs — Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully terminated.

--ignorefailure =[true|false] — If true, the installation is considered a success even if the `%post` script terminated with an error.

%firstboot

Creates an `init` script that runs only during the first boot. The script has no effect on subsequent boots. If multiple `%firstboot` sections are specified, they run in the order that they appear in the kickstart file.

NOTE You cannot check the semantics of `%firstboot` scripts until the system is booting for the first time. A `%firstboot` script might contain potentially catastrophic errors that are not exposed until after the installation is complete.

--interpreter =[python|busybox] — Specifies an interpreter to use. The default is busybox.

NOTE You cannot check the semantics of the `%firstboot` script until the system boots for the first time. If the script contains errors, they are not exposed until after the installation is complete.

Differences Between ESXi 4.x and ESXi 5.0 Scripted Installation and Upgrade Commands

Before you perform a scripted ESXi installation or upgrade, if you are familiar with ESXi version 4.x scripted installation, note the differences between ESXi 4.x and ESXi 5.0 scripted installation and upgrade commands.

In ESXi 5.0, because the installation image is loaded directly into the host RAM when the host boots, you do not need to include the location of the installation media in the installation script.

ESXi 5.0 supports scripted upgrades in addition to scripted installation.

Command differences are noted in the following summary.

`accepteula` or `vmaccepteula`	Only in ESXi
`autopart`	Deprecated and replaced with `install`, `upgrade`, or `installorupgrade`.
`auth` or `authconfig`	Not supported in ESXi 5.0.
`bootloader`	Not supported in ESXi 5.0.
`esxlocation`	Deprecated and unused in ESXi.
`firewall`	Not supported in ESXi 5.0.
`firewallport`	Not supported in ESXi 5.0.
`install`, `installorupgrade`, `upgrade`	These commands replace the deprecated autopart command. Use one of these command to specify the disk to partition, and the `part` command to create the vmfs datastore. `installorupgrade` and `upgrade` are newly supported in ESXi 5.0.
`serialnum` or `vmserialnum`	Deprecated in ESXi 5.0. You can license the host only after installation.
`timezone`	Not supported in ESXi 5.0.
`virtualdisk`	Not supported in ESXi 5.0.
`zerombr`	Not supported in ESXi 5.0.
`%firstboot`	`--level` option not supported in ESXi 5.0.
`%packages`	Not supported in ESXi 5.0.

Disk Device Names

The `install`, `upgrade`, and `installorupgrade` installation script commands require the use of disk device names.

Table 6-6. Disk Device Names

Format	Examples	Description
VML	vml.00025261	The device name as reported by the vmkernel
MPX	mpx.vmhba0:C0:T0:L0	The device name

NOTE When you use a scripted upgrade to upgrade from ESX 4.x to ESXi 5.0, the MPX and VML disk names change, which might cause the upgrade to fail. To avoid this problem, use Network Address Authority Identifiers (NAA IDs) for the disk device instead of MPX and VML disk names.

About the boot.cfg File

The boot loader configuration file `boot.cfg` specifies the kernel, the kernel options, and the boot modules that the `mboot.c32` boot loader uses in an ESXi installation.

The `boot.cfg` file is provided in the ESXi installer. You can modify the `kernelopt` line of the `boot.cfg` file to specify the location of an installation script or to pass other boot options.

The `boot.cfg` file has the following syntax:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

The commands in `boot.cfg` configure the boot loader.

Table 6-7. Commands in `boot.cfg` .

Command	Description
`title=STRING`	Sets the boot loader title to *STRING*.
`kernel=FILEPATH`	Sets the kernel path to *FILEPATH*.
`kernelopt=STRING`	Appends *STRING* to the kernel boot options.
`modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn`	Lists the modules to be loaded, separated by three hyphens (---).

See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 88, "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 92, "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 94, and "PXE Booting the ESXi Installer," on page 89.

Install, Upgrade, or Migrate ESXi from a CD or DVD Using a Script

You can install, upgrade, or migrate ESXi from a CD/DVD drive using a script that specifies the installation or upgrade options.

You can start the installation or upgrade script by entering a boot option when you start the host. You can also create an installer ISO image that includes the installation script. With an installer ISO image, you can perform a scripted, unattended installation when you boot the resulting installer ISO image. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 88.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Prerequisites

Before you run the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

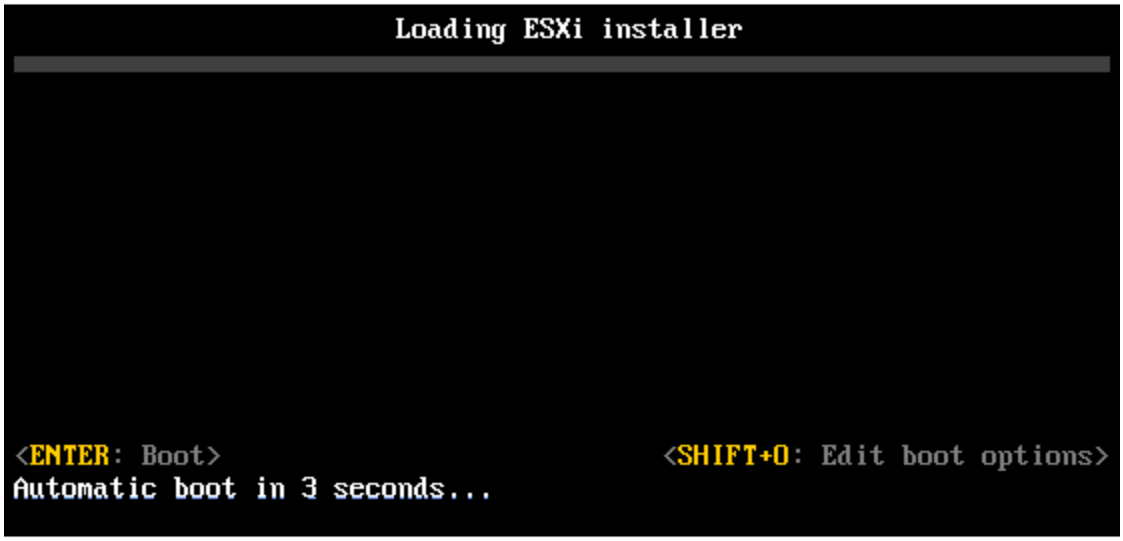
- The system on which you are installing, upgrading, or migrating meets the hardware requirements. See "ESXi Hardware Requirements," on page 13.

- You have the ESXi installer ISO on an installation CD/DVD. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 85.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See "About Installation and Upgrade Scripts," on page 114.
- You have selected a boot command to run the scripted installation, upgrade or migration. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 112. For a complete list of boot commands, see "Boot Options," on page 113.

Procedure

1 Boot the ESXi installer from the CD or DVD using the local CD/DVD-ROM drive.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

The boot option has the form `ks=`.

4 Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Install, Upgrade, or Migrate ESXi from a USB Flash Drive Using a Script

You can install, upgrade, or migrate ESXi from a USB flash drive using a script that specifies the installation or upgrade options.

IMPORTANT After you upgrade or migrate your host to ESXi 5.0, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Supported boot options are listed in "Boot Options," on page 113.

Prerequisites

Before running the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

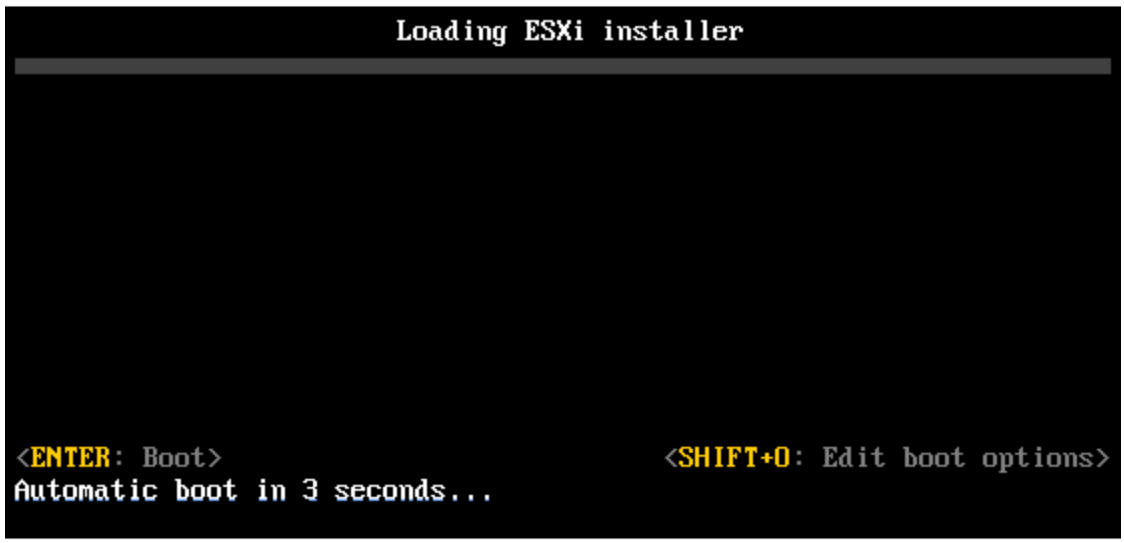
- The system that you are installing, upgrading, or migrating to ESXi meets the hardware requirements for the installation or upgrade. See "ESXi Hardware Requirements," on page 13.

- You have the ESXi installer ISO on a bootable USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 86.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See "About Installation and Upgrade Scripts," on page 114.
- You have selected a boot option to run the scripted installation, upgrade, or migration. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 112.

Procedure

1 Boot the ESXi installer from the USB flash drive.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

The boot option has the form `ks=`.

4 Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Performing a Scripted Installation or Upgrade of ESXi by PXE Booting the Installer

ESXi 5.0 provides many options for PXE booting the installer and using an installation or upgrade script.

- For information about setting up a PXE infrastructure, see "PXE Booting the ESXi Installer," on page 89.
- For information about creating and locating an installation script, see "About Installation and Upgrade Scripts," on page 114.
- For specific procedures to PXE boot the ESXi installer and use an installation script, see one of the following topics:
  - "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 94
  - "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 92
  - "PXE Boot the ESXi Installer Using gPXE," on page 95

- For information about using Auto Deploy to perform a scripted upgrade by PXE booting, see "Using vSphere Auto Deploy to Reprovision Hosts," on page 125.

Using vSphere Auto Deploy to Reprovision Hosts

If a host was deployed using vSphere Auto Deploy, you can use Auto Deploy to reprovision the host with a new image profile that contains an ESXi upgrade. You can use vSphere ESXi Image Builder PowerCLI to create and manage image profiles.

These instructions assume that you are reprovisioning a host that has already been provisioned with Auto Deploy. Provisioning a host that has never been provisioned with Auto Deploy differs from the process described here to upgrade a host. For information about using vSphere Auto Deploy and ESXi Image Builder PowerCLI, see the information about using vSphere Auto Deploy and vSphere ESXi Image Builder CLI in the *vSphere Installation and Setup* documentation.

Reprovisioning Hosts

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image or a different host profile.

A first boot using Auto Deploy requires that you set up your environment and add rules to the rule set. See the topic "Preparing for vSphere Auto Deploy" in the *vSphere installation and Setup* documentation.

The following reprovisioning operations are available.

- Simple reboot.
- Reboot of hosts for which the user answered questions during the boot operation.
- Reprovision with a different image profile.
- Reprovision with a different host profile.

Reprovision Hosts with Simple Reboot Operations

A simple reboot of a host that is provisioned with Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, and vCenter Server location.

Setup includes DHCP server setup, writing rules, and making an image available to the Auto Deploy infrastructure.

Prerequisites

Make sure the setup you performed during the first boot operation is in place.

Procedure

1 Check that the image profile and host profile for the host are still available, and that the host has the identifying information (asset tag, IP address) it had during previous boot operations.

2 Place the host in maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

3 In the vSphere Client, right-click the host and choose **Reboot**.

The host shuts down. When the host reboots, it uses the image profile that the Auto Deploy server provides. The Auto Deploy server also applies the host profile stored on the vCenter Server system.

Reprovision a Host with a New Image Profile

You can reprovision the host with a new image profile, host profile, or vCenter Server location by changing the rule for the host and performing a test and repair operation.

Several options for reprovisioning hosts exist.

- If the VIBs that you want to use support live update, you can use an `esxcli software vib` command. In that case, you must also update the rule set to use an image profile that includes the new VIBs upon reboot.
- During testing, you can to apply an image profile to an individual host with the `Apply-EsxImageProfile` cmdlet and reboot the host so the change takes effect. The `Apply-EsxImageProfile` cmdlet updates the association between the host and the image profile but does not install VIBs on the host.
- In all other cases, use this procedure.

Prerequisites

- Create the image profile you want boot the host with. Use the Image Builder PowerCLI. See "Using vSphere ESXi Image Builder CLI" in the *vSphere Installation and Setup* documentation.
- Make sure that the setup that you performed during the first boot operation is in place.

Procedure

1 At the PowerShell prompt, run the `Connect-VIServer` PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

```
Connect-VIServer myVCServer
```

The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2 Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with the Image Builder PowerCLI.

3 Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run **Add-EsxSoftwareDepot *depot_url***.
ZIP file	a Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine. b Run **Add-EsxSoftwareDepot C:*file_path**my_offline_depot*.zip**.

4 Run `Copy-DeployRule` and specify the `ReplaceItem` parameter to change the rule that assigns an image profile to hosts.

The following cmdlet replaces the current image profile that the rule assigns to the host with the *my_new_imageprofile* profile. After the cmdlet completes, `myrule` assigns the new image profile to hosts. The old version of `myrule` is renamed and hidden.

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

5 Test and repair rule compliance for each host that you want to deploy the image to.

See "Test and Repair Rule Compliance," on page 128.

When you reboot hosts after compliance repair, Auto Deploy provisions the hosts with the new image profile.

Applying a Host Profile to Prompt for User Input

If a host required user input during a previous boot, the answers are saved with the vCenter Server in an answer file. If you want to prompt the user for new information, you reapply the host profile.

Prerequisites

Attach a host profile that prompts for user input to the host.

Procedure

1 Place the host in maintenance mode. Migrate all virtual machines to different hosts, and place the host into maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

2 In the vSphere Client, choose **Host Profiles > Apply Profile** and choose the host profile that requires user input when prompted.

3 When prompted, provide the user input.

You can now direct the host to exit maintenance mode.

The user input information is saved in an answer file. The next time you boot, the answer file information is applied to the host. One answer file per host is available.

Assign a Host Profile to Hosts

Auto Deploy can assign a host profile to one or more hosts. The host profile might include information about storage configuration, network configuration, or other characteristics of the host. If you add a host to a cluster, that cluster's host profile is used.

The following procedure explains how to write a rule that assigns a host profile to hosts. To assign the host profiles to hosts already provisioned with Auto Deploy, you must also perform a test and repair cycle. See "Test and Repair Rule Compliance," on page 128.

In many cases, you assign a host to a cluster instead of specifying a host profile explicitly. The host uses the host profile of the cluster.

Prerequisites

- Install vSphere PowerCLI and all prerequisite software.
- Export the host profile that you want to use.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See the information about using Auto Deploy Cmdlets in the *vSphere Installation and Setup* documentation.

Procedure

1 Run the `Connect-VIServer` PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

```
Connect-VIServer 192.XXX.X.XX
```

The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2 In the vSphere Client, select **View > Management > Host Profiles** to display the Host Profiles panel and export the host profile that you want to use from there.

3 Find the name of the host profile by running `Get-VMhostProfile`, passing in the server on which the host profile is located.

4 At the PowerCLI prompt, define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the host profile.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

The specified item is assigned to all hosts with the specified attributes. This example specifies a rule named testrule2. The rule assigns the specified host profile my_host_profile to all hosts with an IP address inside the specified range and with a manufacturer of Acme or Zven.

5 Add the rule to the rule set.

```
Add-DeployRule testrule2
```

By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

What to do next

- Upgrade existing hosts to use the new host profile by performing compliance test and repair operations on those hosts. See "Test and Repair Rule Compliance," on page 128.
- Turn on unprovisioned hosts to provision them with the host profile.

Test and Repair Rule Compliance

When you add a rule to the Auto Deploy rule set or make changes to one or more rules, hosts are not updated automatically. Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

This task assumes that your infrastructure includes one or more ESXi hosts provisioned with Auto Deploy, and that the host on which you installed VMware PowerCLI can access those ESXi hosts.

Prerequisites

- Install VMware PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See the information about using Auto Deploy Cmdlets in the *vSphere Installation and Setup* documentation.

Procedure

1 Use PowerCLI to check which Auto Deploy rules are currently available.

```
Get-DeployRule
```

The system returns the rules and the associated items and patterns.

2 Make a change to one of the available rules, for example, you might change the image profile and the name of the rule.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

You cannot edit a rule already added to a rule set. Instead, you copy the rule and replace the item or pattern you want to change.

3 Verify that the host that you want to test rule set compliance for is accessible.

```
Get-VMHost -Name MyEsxi42
```

4 Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

5 Examine the differences between what is in the rule set and what the host is currently using.

```
$tr.itemlist
```

The system returns a table of current and expected items.

```
CurrentItem                          ExpectedItem
-----------                          ------------
My Profile 25                        MyProfileUpdate
```

6 Remediate the host to use the revised rule set the next time you boot the host.

```
Repair-DeployRuleSetCompliance $tr
```

What to do next

If the rule you changed specified the inventory location, the change takes effect when you repair compliance. For all other changes, boot your host to have Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

Upgrading Hosts by Using esxcli Commands

Using the vSphere CLI, you can patch ESXi 5.0 hosts.

You cannot use `esxcli` commands to upgrade version 4.x ESX or ESXi hosts to ESXi 5.0. To upgrade version 4.x ESX or ESXi hosts to ESXi 5.0, use vSphere Update Manager, or perform an interactive or scripted upgrade.

To use esxcli vCLI commands, you must install vSphere CLI (vCLI). For more information about installing and using the vSphere CLI, see the following documents:

- *Getting Started with vSphere Command-Line Interfaces*
- *vSphere Command-Line Interface Concepts and Examples*
- *vSphere Command-Line Interface Reference* is a reference to `vicfg-` and related vCLI commands.

NOTE If you press Ctrl+C while an `esxcli` command is running, the command-line interface exits to a new prompt without displaying a message. However, the command continues to run to completion.

For ESXi hosts deployed with vSphere Auto Deploy, the tools VIB must be part of the base booting image used for the initial Auto Deploy installation. The tools VIB cannot be added separately later.

VIBs, Image Profiles, and Software Depots

Upgrading ESXi with esxcli commands requires an understanding of VIBs, image profiles, and software depots.

The following technical terms are used throughout the vSphere documentation set in discussions of installation and upgrade tasks.

VIB — A VIB is an ESXi software package. VMware and its partners package solutions, drivers, CIM providers, and applications that extend the ESXi platform as VIBs. VIBs are available in software depots. You can use VIBs to create and customize ISO images or to upgrade ESXi hosts by installing VIBs asynchronously onto the hosts.

Image Profile — An image profile defines an ESXi image and consists of VIBs. An image profile always includes a base VIB, and might include more VIBs. You examine and define an image profile using the Image Builder PowerCLI.

Software Depot — A software depot is a collection of VIBs and image profiles. The software depot is a hierarchy of files and folders and can be available through an HTTP URL (online depot) or a ZIP file (offline depot). VMware and VMware partners make depots available. Companies with large VMware installations might create internal depots to provision ESXi hosts with vSphere Auto Deploy, or to export an ISO for ESXi installation.

Understanding Acceptance Levels for VIBS and Hosts

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host.

The acceptance level applies to individual VIBs installed by using the `esxcli software vib install` and `esxcli software vib update` commands, to VIBs installed using vSphere Update Manager, and to VIBs in image profiles.

The acceptance level of all VIBs on a host must be at least as high as the host acceptance level. For example, if the host acceptance level is VMwareAccepted, you can install VIBs with acceptance levels of VMwareCertified and VMwareAccepted, but you cannot install VIBs with acceptance levels of PartnerSupported or CommunitySupported. To install a VIB with a less restrictive acceptance level than that of the host, you can change the acceptance level of the host by using the vSphere Client or by running `esxcli software acceptance` commands.

Setting host acceptance levels is a best practice that allows you to specify which VIBs can be installed on a host and used with an image profile, and the level of support you can expect for a VIB. For example, a CommunitySupported VIB might not be recommended for an ESXi server in a production environment.

VMware supports the following acceptance levels.

VMwareCertified — The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only IOVP drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.

VMwareAccepted — VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plugins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

PartnerSupported VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

CommunitySupported The Community Supported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Table 6-8. VIB Acceptance Levels Required to Install on Hosts

Host Acceptance Level	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
VMwareCertified	x			
VMwareAccepted	x	x		
PartnerSupported	x	x	x	
CommunitySupported	x	x	x	x

Match a Host Acceptance Level with an Update Acceptance Level

You can change the host acceptance level to match the acceptance level for a VIB or image profile that you want to install. The acceptance level of all VIBs on a host must be at least as high as the host acceptance level.

Use this procedure to determine the acceptance levels of the host and the VIB or image profile to install, and to change the acceptance level of the host, if necessary for the update.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Procedure

1 Retrieve the acceptance level for the VIB or image profile.

Option	Description
List information for all VIBs	**`esxcli --server=`*`server_name`*` software sources vib list --depot=`*`depot_URL`***
List information for a specified VIB	**`esxcli --server=`*`server_name`*` software sources vib list --viburl=`*`vib_URL`***
List information for all image profiles	**`esxcli --server=`*`server_name`*` software sources profile list --depot=`*`depot_URL`***
List information for a specified image profile	**`esxcli --server=`*`server_name`*` software sources profile get --depot=`*`depot_URL`*` --profile=`*`profile_name`***

2 Retrieve the host acceptance level.

```
esxcli --server=server_name software acceptance get
```

3 (Optional) If the acceptance level of the VIB is more restrictive than the acceptance level of the host, change the acceptance level of the host.

```
esxcli --server=server_name software acceptance set --level=acceptance_level
```

The *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

NOTE You can use the `--force` option for the `esxcli software vib` or `esxcli software profile` command to add a VIB or image profile with a lower acceptance level than the host. A warning will appear. Because your setup is no longer consistent, the warning is repeated when you install VIBs, remove VIBs, and perform certain other operations on the host.

Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted

VIBs that you can install with live install do not require the host to be rebooted, but might require the host to be placed in maintenance mode. Other VIBs and profiles might require the host to be rebooted after the installation or update.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Procedure

1 Check whether the VIB or image profile that you want to install requires the host to be placed in maintenance mode or to be rebooted after the installation or update.

Run one of the following commands.

Option	Description
Check the VIB	**`esxcli --server=server_name software sources vib get -v path_to_vib`**
Check the VIBs in a depot	**`esxcli --server=server_name software sources vib get --depot=depot_name`**
Check the image profile in a depot	**`esxcli --server=server_name software sources profile get --depot=depot_name`**

2 Review the return values.

The return values, which are read from the VIB metadata, indicate whether the host must be in maintenance mode before installing the VIB or image profile, and whether installing the VIB or profile requires the host to be rebooted.

NOTE vSphere Update Manager relies on the `esxupdate`/`esxcli` scan result to determine whether maintenance mode is required or not. After a VIB is installed on a live system, if `Live-Install-Allowed` and `Live-Remove-Allowed` are both set to false, the installation result will instruct Update Manager to reboot the host. During the reboot, Update Manager will automatically put the host into maintenance mode.

What to do next

If necessary, place the host in maintenance mode. See "Place a Host in Maintenance Mode," on page 133. If a reboot is required, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster before the installation or update.

Place a Host in Maintenance Mode

Some installation and update operations that use live install require the host to be in maintenance mode.

To determine whether an upgrade operation requires the host to be in maintenance mode, see "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 132

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Check to determine whether the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

2 Run one of the following commands for each virtual machine to power off all virtual machines running on the ESXi host.

Option	Command
To have the system try to shut down the guest operating system	`vmware-cmd --server=server_name path_to_vm stop soft`
To force the power off operation	`vmware-cmd --server=server_name path_to_vm stop hard`

Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

3 Place the host in maintenance mode.

```
vicfg-hostops --server=server_name --operation enter
```

4 Verify that the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

Update a Host with Individual VIBs

You can update a host with VIBs stored in a software depot that is accessible through a URL or in an offline ZIP depot.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 132. See "Place a Host in Maintenance Mode," on page 133.

- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

1 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

2 Find out which VIBs are available in the depot.

Option	Description
from a depot accessible by URL	`esxcli --server=server_name software sources vib list --depot=http://web_server/depot_name`
from a local depot ZIP file	`esxcli --server=server_name software sources vib list --depot=path_to_depot_zip_file/depot_ZIP_file`

You can specify a proxy server by using the `--proxy` argument.

3 Update the existing VIBs to include the VIBs in the depot or install new VIBs.

Option	Description
Update VIBs from a depot accessible by URL	`esxcli --server=server_name software vib update --depot=http://web_server/depot_name`
Update VIBs from a local depot ZIP file	`esxcli --server=server_name software vib update --depot=path_to_depot_ZIP_file/depot_ZIP_file`
Install all VIBs from a ZIP file on a specified offline depot (includes both VMware VIBs and partner-supplied VIBs)	`esxcli --server=server_name software vib install --depot path_to_VMware_vib_ZIP_file\VMware_vib_ZIP_file --depot path_to_partner_vib_ZIP_file\partner_vib_ZIP_file`

Options for the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *esxcli Reference* at http://www.vmware.com/support/developer/vcli/.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

Update a Host with Image Profiles

You can update a host with image profiles stored in a software depot that is accessible through a URL or in an offline ZIP depot.

When you specify a target server by using `--server=server_name` in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

NOTE Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 132. See "Place a Host in Maintenance Mode," on page 133.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

1 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

2 Determine which image profiles are available in the depot.

```
esxcli --server=server_name software sources profile list --depot=http://webserver/depot_name
```

You can specify a proxy server by using the `--proxy` argument.

3 Update the existing image profile to include the VIBs or install new VIBs.

IMPORTANT The `software profile update` command updates existing VIBS with the corresponding VIBs from the specified profile, but does not affect other VIBs installed on the target server. The `software profile install` command installs the VIBs present in the depot image profile, and removes any other VIBS installed on the target server.

Option	Description
Update the image profile from a depot accessible by URL	`esxcli --server=server_name software profile update --depot=http://webserver/depot_name --profile=profile_name`
Update the image profile from ZIP file stored locally on the target server	`esxcli --server=server_name software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=profile_name`
Update the image profile from a ZIP file on the target server, copied into a datastore	`esxcli --server=server_name software profile update --depot="[datastore_name]profile_ZIP_file" --profile=profile_name`
Update the image profile from a ZIP file copied locally and applied on the target server	`esxcli --server=server_name software profile update --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name`
Install all new VIBs in a specified profile accessible by URL	`esxcli --server=server_name software profile install --depot=http://webserver/depot_name --profile=profile_name`
Install all new VIBs in a specified profile from a ZIP file stored locally on the target	`esxcli --server=server_name software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=profile_name`
Install all new VIBs from a ZIP file on the target server, copied into a datastore	`esxcli --server=server_name software profile install --depot="[datastore_name]profile_ZIP_file" --profile=profile_name`
Install all new VIBs from a ZIP file copied locally and applied on the target server	`esxcli --server=server_name software profile install --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name`

NOTE Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

Update Hosts with Third-Party ZIP Files

You can update hosts with third-party VIBs or image profiles only by downloading a ZIP file of a depot that is prepared by the VMware partner directly to the ESXi host.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

When you specify a target server by using `--server=server_name` in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Download the ZIP file of a depot bundle prepared by the third-party VMware partner.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 132. See "Place a Host in Maintenance Mode," on page 133.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

- Install the ZIP file.

  ```
  esxcli --server=server_name software vib update --
  depot=/path_topartner_vib_ZIP/partner_ZIP_file_name.zip
  ```

Remove VIBs from a Host

You can uninstall third-party VIBs or VMware VIBs from your ESXi host.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Prerequisites

- If the removal requires a reboot, and if the host belongs to a VMware HA cluster, disable HA for the host.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 132. See "Place a Host in Maintenance Mode," on page 133.
- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Run one of the following commands for each virtual machine to power off all virtual machines running on the ESXi host.

Option	Command
To have the system try to shut down the guest operating system	`vmware-cmd --server=server_name path_to_vm stop soft`
To force the power off operation	`vmware-cmd --server=server_name path_to_vm stop hard`

Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

2 Place the host in maintenance mode.

```
vicfg-hostops --server=server_name --operation enter
```

3 If necessary, shut down or migrate virtual machines.

4 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

5 Remove the VIB.

```
esxcli --server=server_name software vib remove --vibname=name
```

Specify one or more VIBs to remove in one of the following forms:

- *name*
- *name*:*version*
- *vendor*:*name*
- *vendor*:*name*:*version*

For example, the command to remove a VIB specified by vendor, name and version would take this form:

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

NOTE The `remove` command supports several more options. See the *vSphere Command-Line Interface Reference*.

Adding Third-Party Extensions to Hosts with esxcli

If a third-party extension is released as a VIB package, and you use the `esxcli software vib` command to add the VIB package to your system, the VIB system updates the firewall ruleset and refreshes the host daemon after you reboot your system.

Otherwise, you can use a firewall configuration file to specify port rules for host services that you want to enable for the extension. The *vSphere Security* documentation discusses how to add, apply, and refresh a firewall rule set and lists the `esxcli network firewall` commands.

The ESXi 5.0 `ruleset.xml` format for ESXi 5.0 is the same as in version 4.x for ESX and ESXi, but has two more tags, `enabled` and `required`. The ESXi 5.0 firewall still supports the older format.

Perform a Dry Run of an esxcli Installation or Upgrade

You can use the `--dry-run` option to preview the results of an installation or upgrade operation. A dry run of the installation or update procedure does not make any changes, but reports the VIB-level operations that will be performed if you run the command without the `--dry-run` option.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter the installation or upgrade command, adding the **--dry-run** option.

- **`esxcli --server=`*`server_name`*` software vib install --dry-run`**
- **`esxcli --server=`*`server_name`*` software vib update --dry-run`**
- **`esxcli --server=`*`server_name`*` software profile install --dry-run`**
- **`esxcli --server=`*`server_name`*` software profile update --dry-run`**

2 Review the output that is returned.

The output shows which VIBs will be installed or removed and whether the installation or update requires a reboot.

Display the Installed VIBs and Profiles That Will Be Active After the Next Host Reboot

You can use the `--rebooting-image` option to list the VIBs and profiles that are installed on the host and will be active after the next host reboot.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter one of the following commands.

Option	Description
For VIBs	**`esxcli --server=`*`server_name`*` software vib list --rebooting-image`**
For Profiles	**`esxcli --server=`*`server_name`*` software profile get --rebooting-image`**

2 Review the output that is returned.

The output displays information for the ESXi image that will become active after the next reboot. If the pending-reboot image has not been created, the output returns nothing.

Display the Image Profile and Acceptance Level of the Host

You can use the `software profile get` command to display the currently installed image profile and acceptance level for the specified host.

This command also shows details of the installed image profile history, including profile modifications.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting , run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter the following command.

```
esxcli --server=server_name software profile get
```

2 Review the output.

Errors and Warnings Returned by the Installation and Upgrade Precheck Script

The installation and upgrade precheck script runs tests to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

Table 6-9. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script

Error or Warning	Description
64BIT_LONGMODESTATUS	The host processor must be 64-bit.
COS_NETWORKING	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning will be output for each such occurrence.
CPU_CORES	The host must have at least two cores.
DISTRIBUTED_VIRTUAL_SWITCH	If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the test checks to make sure the upgrade also contains the VEM software, and that it supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the test returns a warning, and the result indicates which version of the VEM software was expected on the upgrade ISO and which version, if any, were found. You can use ESXi Image Builder CLI to create a custom installation ISO that includes the appropriate version of the VEM software.

Table 6-9. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (Continued)

Error or Warning	Description
HARDWARE_VIRTUALIZATION	Warning. If the host processor doesn't have hardware virtualization or if hardware virtualization is not turned on in the host BIOS, host performance will suffer. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation.
MD5_ROOT_PASSWORD	This test checks that the root password is encoded in MD5 format. If a password is not encoded in MD5 format, it might be significant only to eight characters. In this case, any characters after the first eight are no longer authenticated after the upgrade, which can create a security issue. To work around this problem, see VMware Knowledge Base article 1024500.
MEMORY_SIZE	The host requires the specified amount of memory to upgrade.
PACKAGE_COMPLIANCE	vSphere Update Manager only. This test checks the existing software on the host against the software contained on the upgrade ISO to determine whether the host has been successfully upgraded. If any of the packages are missing or are an older version than the package on the upgrade ISO, the test returns an error and indicates which software was found on the host, and which software was found on the upgrade ISO.
PARTITION_LAYOUT	Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200
POWERPATH	This test checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the test checks to make sure that matching components (CIM, vmkernel module) also exist in the upgrade. If they do not, the test returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found.
PRECHECK_INITIALIZE	This test checks that the precheck script itself can be run.
SANE_ESX_CONF	The file `/etc/vmware/esx.conf` must exist on the host.
SPACE_AVAIL_ISO	vSphere Update Manager only. The host disk must have enough free space to store the contents of the installer CD or DVD.
SPACE_AVAIL_CONFIG	vSphere Update Manager only. The host disk must have enough free space to store the 4.x configuration between reboots.
SUPPORTED_ESX_VERSION	Upgrading or migration to ESXi 5.0 is possible only from version 4.x ESXi or ESX hosts.
TBOOT_REQUIRED	This message applies only to vSphere Update Manager upgrades. The upgrade fails with this error when the host system is running in Trusted Boot mode (tboot), but the ESXi upgrade ISO does not contain any tboot VIBs. This test prevents an upgrade that can make the host less secure.

Table 6-9. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (Continued)

Error or Warning	Description
UNSUPPORTED_DEVICES	Warning. This test checks for unsupported devices. Some PCI devices are not supported in ESXi 5.0.
UPDATE_PENDING	This test checks the 4.x host for VIB installations that require a reboot. This test fails if one or more such VIBs is installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to reliably determine which packages are currently installed on the host, so it might not be safe to rely on the rest of the precheck tests to determine whether an upgrade is safe. If you encounter this error, restart the host and retry the upgrade.

After You Upgrade or Migrate Hosts

A host upgrade or migration is not complete until you have ensured that the host is reconnected to its managing vCenter Server and reconfigured if necessary, and that the host license is reapplied or upgraded.

After you upgrade or migrate a host, take the following actions:

- View the upgrade logs. You can use the vSphere Client to export the log files.
- If vCenter Server manages the host, you must reconnect the host to vCenter Server by right-clicking the host in the vCenter Server inventory and selecting **Connect**.
- When the upgrade is complete, ESXi is in evaluation mode. The evaluation mode period is 60 days. You must reapply your license or assign an upgraded license to your product within 60 days after the upgrade. Use the License Portal and the vSphere Client to configure licensing. See
- On the VMware Web site, log in to your account page to access the license portal. From the license portal, upgrade your ESXi license. Use the vSphere Client to assign the upgraded license key to the host.
- The host sdX devices might be renumbered after the upgrade. If necessary, update any scripts that reference sdX devices.
- After the upgrade, convert any ESX 3.x-style /adv/Disk/MaskLUNs LUN masks to the claim rule format. Run the `esxcli storage core claimrule convert` command in the vSphere Command-Line Interface (vCLI). This command converts the `/adv/Disk/MaskLUNs` advanced configuration entry in `/etc/vmware/esx.conf` to claim rules with MASK_PATH as the plug-in.

CAUTION This conversion will not work for all input MaskLUNs variations. See the *vSphere Command-Line Interface Reference*.

- Upgrade virtual machines on the host. See Chapter 7, "Upgrading Virtual Machines," on page 143.

About ESXi Evaluation and Licensed Modes

After you purchase a host license, VMware provides a serial number that you can use to license vSphere. You can use evaluation mode to access the full ESXi feature set, including features you have not purchased a license for.

For example, in evaluation mode, you can use vMotion, HA, DRS, and other features, even if you have not licensed those features.

The installable version of ESXi is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal USB device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host, even if you start in licensed mode rather than evaluation mode. Any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. To take full advantage of the 60-day evaluation period, you should convert to evaluation mode as soon as possible after you first power on the host. See "Convert an ESXi Host to Evaluation Mode," on page 142.

For information about licensing the host, see the *vCenter Server and Host Management*.

Reapplying Licenses After Upgrading to ESXi 5.0

After you upgrade to ESXi 5.0, reapply your host license.

After upgrading, your ESXi 5.0 software returns to evaluation mode until you reapply your license. If you used part of the 60-day evaluation period before upgrading, the time remaining in your evaluation period is decreased by the amount already used. For example, if you used 20 days of the evaluation period before upgrading, your remaining evaluation period after the upgrade is 40 days. See "About ESXi Evaluation and Licensed Modes," on page 141.

You can apply your license using the vSphere Client and vCenter Server. See the *vCenter Server and Host Management* documentation.

Convert an ESXi Host to Evaluation Mode

You can switch a licensed ESXi host to evaluation mode to explore all the features of ESXi, including features that you have not licensed.

See "About ESXi Evaluation and Licensed Modes," on page 141.

Prerequisites

The 60-day evaluation period has not expired.

Procedure

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

2 Click the **Configuration** tab.

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

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

5 Click **(No License Key)**.

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

You can now access all the features of ESXi.

Upgrading Virtual Machines 7

After you perform an ESX/ESXi upgrade, VMware recommends that you upgrade all the virtual machines that reside on the host. Upgrading virtual machines ensures that they remain compatible with the upgraded host software, and can take advantage of new features.

The first step in upgrading virtual machines is to upgrade VMware Tools. If the virtual machines do not have VMware Tools installed, you can use the VMware Tools upgrade procedure to install VMware Tools. After you install or upgrade VMware Tools, upgrade the virtual machine hardware.

NOTE Do not use `vmware-vmupgrade.exe` to upgrade virtual machines.

VMware offers the following tools for upgrading virtual machines:

vSphere Client	Requires you to perform the virtual machine upgrade one step at a time, but does not require vSphere Update Manager.
vSphere Update Manager	Automates the process of upgrading and patching virtual machines, thereby ensuring that the steps occur in the correct order. You can use Update Manager to directly upgrade virtual machine hardware, VMware Tools, and virtual appliances. You can also patch and update third-party software running on the virtual machines and virtual appliances. See "Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager," on page 147 and the *Installing and Administering VMware vSphere Update Manager*documentation.

This chapter includes the following topics:

- "About VMware Tools," on page 144
- "About Virtual Machines and Host Upgrades," on page 145
- "Virtual Machine Hardware Versions," on page 146
- "Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager," on page 147
- "Planning Downtime for Virtual Machines," on page 152
- "Downtime for Upgrading Virtual Machines," on page 152
- "Manually Install or Upgrade VMware Tools in a Windows Virtual Machine," on page 153
- "Manually Install or Upgrade VMware Tools in a Linux Virtual Machine," on page 154
- "Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine," on page 156
- "Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine," on page 157
- "Operating System Specific Packages for Linux Guest Operating Systems," on page 158

- "Perform an Automatic Upgrade of VMware Tools," on page 158
- "Upgrade VMware Tools on Multiple Virtual Machines," on page 159
- "Configure a Virtual Machine to Upgrade VMware Tools Automatically," on page 160
- "Upgrade Virtual Hardware," on page 160
- "Upgrade Virtual Hardware on Multiple Virtual Machines," on page 162
- "Uninstall VMware Tools," on page 162

About VMware Tools

VMware Tools improves the performance and management of the virtual machine.

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

- Significantly faster graphics performance and Windows Aero on operating systems that support Aero
- Copying and pasting text, graphics, and files between the virtual machine and the host or client desktop
- Improved mouse performance
- Synchronization of the clock in the virtual machine with the clock on the host or client desktop
- Scripting that helps automate guest operating system operations

Although the guest operating system can run without VMware Tools, many VMware features are not available until you install VMware Tools. For example, if you do not have VMware Tools installed in your virtual machine, you cannot use the shutdown or restart options from the toolbar. You can use only the power options.

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

For complete information about VMware Tools, see *Installing and Configuring VMware Tools*.

Upgrading VMware Tools

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

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

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

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

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

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

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

You have options for upgrading many virtual machines at the same time.

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

For best performance and the latest updates, install or upgrade VMware Tools to the VMware Tools version that is included with the VMware product you are using. Other compatibility options are also available.

- The version of VMware Tools included in vSphere 5.0 is supported on vSphere 4.x and 5.0 virtual machines. That is, you can also use this new version of VMware Tools in virtual machines on ESX/ESXi 4.x hosts.
- Virtual machines in a vSphere 5.0 environment support the versions of VMware Tools included in vSphere 4.0-5.0. That is, you are not strictly required to upgrade VMware Tools if VMware Tools was installed from an ESX/ESXi 4.x host.

About Virtual Machines and Host Upgrades

Some virtual machines that you create on ESXi 5.0 hosts are supported on hosts running earlier versions of ESX/ESXi software.

If you create a virtual machine on an ESXi 5.0 host and select the typical path, the virtual hardware version is version 8. Virtual machines with virtual hardware version 8 are not supported on hosts running versions of ESX/ESXi software earlier than ESXi 5.0. When you create virtual machines on ESXi 5.0 hosts, to ensure that your virtual machines can run on version 4.x ESX and ESXi hosts, select the custom path and select virtual hardware version 7. Virtual machines that have virtual hardware version 7 work properly on ESX/ESXi 4.x hosts and ESXi 5.0 hosts, and you can use vMotion to migrate virtual hardware version 7 virtual machines between between ESX/ESXi 4.x hosts and ESXi 5.0 hosts.

Because paravirtualization (VMI) is not supported on ESXi 5.0, you cannot move VMI-enabled virtual machines from an ESX 3.x or ESX 4.x/ESXi 4.x host to an ESXi 5.0 host when the virtual machines are powered on. When the VMI-enabled virtual machines are powered off, you can move them from ESX 3.x or ESX 4.x/ESXi 4.x host to ESXi 5.0 hosts and then remove VMI devices from the virtual machines before powering on the virtual machines.

Virtual Machine Hardware Versions

The hardware version of a virtual machine reflects the virtual machine's supported virtual hardware features. These features correspond to the physical hardware available on the ESXi host on which you create the virtual machine. Virtual hardware features include BIOS and EFI, available virtual PCI slots, maximum number of CPUs, maximum memory configuration, and other characteristics typical to hardware.

When you create a virtual machine, you can accept the default hardware version, which corresponds to the host on which you create the virtual machine, or an earlier version. You can use an earlier hardware version in the following situations:

- To standardize testing and deployment in your virtual environment.
- If you do not need the capabilities of the newer version.
- To maintain compatibility with older hosts.

Virtual machines with hardware versions earlier than version 8 can run on ESXi 5.0 hosts, but do not have all the capabilities available in hardware version 8. For example, you cannot use 32 virtual processors or 1011GB of memory in virtual machines with hardware versions earlier than version 8.

The vSphere Web Client or the vSphere Client allows you to upgrade virtual machines only to the latest hardware version. If virtual machines do not have to stay compatible with older ESX/ESXi hosts, you can upgrade them on ESXi 5.0 hosts. In this case, they are upgraded to version 8.

- To maintain virtual machine compatibility with ESX/ESXi 3.5 hosts, upgrade the virtual machine on an ESX/ESXi 3.5 host, which results in a virtual machine upgrade to version 4.
- To maintain virtual machine compatibility with ESX/ESXi 4.x hosts, upgrade the virtual machine on an ESX/ESXi 4.x host, which results in a virtual machine upgrade to version 7.

A virtual machine can have an earlier hardware version than that of the host on which it runs in the following cases:

- You migrate a virtual machine created on an ESX/ESXi 4.x or earlier host to an ESXi 5.0 host.
- You create a virtual machine on an ESXi 5.0 host by using an existing virtual disk that was created on an ESX/ESXi 4.x or earlier host.
- You add a virtual disk created on an ESX/ESXi 4.x or earlier host to a virtual machine created on an ESXi 5.0 host.

You can create, edit, and run different virtual machine versions on a host if the host supports that version. Sometimes, virtual machine actions on a host are limited or the virtual machine has no access to the host.

Table 7-1. ESXi Hosts and Compatible Virtual Machine Hardware Versions

	Version 8	Version 7	Version 4	Compatible with vCenter Server Version
ESXi 5.0	Create, edit, run	Create, edit, run	Edit, run	vCenter Server 5.0
ESX/ESXi 4.x	Not supported	Create, edit, run	Create, edit, run	vCenter Server 4.x
ESX Server 3.x	Not supported	Not supported	Create, edit, run	VirtualCenter Server 2.x and later

Version 3 virtual machines are not supported on ESXi 5.0 hosts. To make full use of these virtual machines, upgrade the virtual hardware.

NOTE Virtual machine hardware version 4 might be listed as VM3 in documentation for earlier versions of ESX/ESXi.

Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager

An orchestrated upgrade of virtual machines allows you to upgrade VMware Tools and the virtual hardware for the virtual machines in your vSphere inventory at the same time. You can perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

Update Manager makes the process of upgrading the virtual machines convenient by providing baseline groups. When you remediate a virtual machine against a baseline group containing the VMware Tools Upgrade to Match Host baseline and the VM Hardware Upgrade to Match Host baseline, Update Manager sequences the upgrade operations in the correct order. As a result, the guest operating system is in a consistent state at the end of the upgrade.

This workflow describes the overall process to perform an orchestrated upgrade of the virtual machines in your vSphere inventory.

Procedure

1 Create a Virtual Appliance Upgrade Baseline on page 147

You upgrade virtual appliances by using a virtual appliance upgrade baseline. You can either use the predefined virtual appliance upgrade baseline, or create custom virtual appliance upgrade baselines.

2 Create a Virtual Machine and Virtual Appliance Baseline Group on page 148

You can combine upgrade baselines in a virtual machine and virtual appliance baseline group.

3 Attach Baselines and Baseline Groups to Objects on page 149

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.

4 Manually Initiate a Scan of Virtual Machines and Virtual Appliances on page 150

To scan virtual machines and virtual appliances in the vSphere inventory immediately, you can manually initiate a scan against attached baselines and baseline groups.

5 View Compliance Information for vSphere Objects on page 150

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

6 Remediate Virtual Machines and Virtual Appliances on page 151

You can manually remediate virtual machines and virtual appliances immediately, or can schedule a remediation at a time that is convenient for you.

Create a Virtual Appliance Upgrade Baseline

You upgrade virtual appliances by using a virtual appliance upgrade baseline. You can either use the predefined virtual appliance upgrade baseline, or create custom virtual appliance upgrade baselines.

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 Baselines pane.

2 Type a name, and optionally, a description of the baseline.

3 Under Baseline Type, select **VA Upgrade**, and click **Next**.

4 On the Upgrade Options page, select **Vendor** and **Appliance** options from the respective drop-down menus.

The options listed in these menus depend on the virtual appliance upgrades that are downloaded in the Update Manager repository. If no upgrades are downloaded in the repository, the available options are **All Vendors** and **All Products**, respectively.

5 Select an option from the **Upgrade To** drop-down menu.

Option	Description
Latest	Upgrades the virtual appliance to the latest version.
A specific version number	Upgrades the virtual appliance to a specific version. This option is available when you select a specific vendor and appliance name.
Do Not Upgrade	Does not upgrade the virtual appliance.

6 Click **Add Rule**.

7 (Optional) Add multiple rules.

a Click **Add Multiple Rules**.

b Select one or all vendors.

c Select one or all appliances.

d Select one **Upgrade To** option to apply to the selected appliances, and click **OK**.

If you create multiple rules to apply to the same virtual appliance, only the first applicable rule in the list is applied.

8 (Optional) Resolve any conflicts within the rules you apply.

a In the Upgrade Rule Conflict window, select whether to keep the existing rules, to use the newly created rules, or to manually resolve the conflict.

b Click **OK**.

9 Click **Next**.

10 On the Ready to Complete page, click **Finish**.

The new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

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.

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.

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**.

Planning Downtime for Virtual Machines

Plan downtime for each virtual machine during the upgrade process. Typically, this downtime occurs during the virtual machine upgrade and the VMware Tools upgrade. Depending on your upgrade plan, some virtual machine downtime might be required during the ESX upgrade.

If an ESX/ESXi host is not managed by vCenter Server, you cannot use vMotion to move virtual machines. The virtual machines must have some downtime when the ESX/ESXi host reboots after upgrade.

You might not have to shut down more than a single virtual machine at any given time. You can stagger virtual machine downtimes to accommodate a schedule convenient to you and your customers.

For example:

- If your virtual machine users are located in diverse time zones, you can prepare by migrating virtual machines to specific hosts to serve a given time zone. This way you can arrange host upgrades so that virtual machine downtime occurs transparently outside business hours for that time zone.
- If your virtual machine users operate around the clock, you can delay downtime for their virtual machines to normally scheduled maintenance periods. You do not need to upgrade any stage within a certain time period. You can take as long as needed at any stage.

Downtime for Upgrading Virtual Machines

When you upgrade virtual machines, the required downtime depends on the guest operating system.

When you upgrade VMware Tools, expect the following downtime:

- No downtime is required for vCenter Server.
- No downtime is required for ESXi hosts.
- You must reboot Microsoft Windows virtual machines at the end of the upgrade procedure, or later, for the upgrade take effect.
- On Windows guest operating systems, you must reboot the virtual machine three times when you upgrade VMware Tools and the virtual hardware.
- For Linux, NetWare, and Solaris guest operating systems, no reboot is required at the end of the procedure.

During the virtual hardware upgrade, you must shut down the virtual machine for all guest operating systems.

Table 7-2 summarizes the downtime required by guest operating system and by upgrade operation.

Table 7-2. Virtual Machine Downtime by Guest Operating System

Guest Operating System	Upgrade VMware Tools	Upgrade Virtual Hardware
Linux	No downtime.	Downtime for shut down and power on of virtual machine.
NetWare		
Solaris		
Microsoft Windows	Downtime for reboot of guest operating system.	

Manually Install or Upgrade VMware Tools in a Windows Virtual Machine

All supported Windows guest operating systems support VMware Tools.

Install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management. When you power on a virtual machine, if a new version of VMware Tools is available, you see a notification in the status bar of the guest operating system.

For Windows 2000 and later, VMware Tools installs a virtual machine upgrade helper tool. This tool restores the network configuration if you upgrade from virtual hardware version 4 to version 7 or higher.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- If the guest operating system is a Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows 7 operating system, log in as an administrator. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows Me guest operating system.

Procedure

1 Select the menu command to mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools

2 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

3 If you are installing VMware Tools for the first time, click **OK** in the Install VMware Tools information screen.

If autorun is enabled for the CD-ROM drive in the guest operating system, the VMware Tools installation wizard appears.

4 If autorun is not enabled, to manually launch the wizard, click **Start > Run** and enter `D:\setup.exe`, where `D:` is your first virtual CD-ROM drive.

5 Follow the on-screen instructions.

To install nondefault components, select the **Custom** setup.

6 If the New Hardware wizard appears, go through the wizard and accept the defaults.

7 If you are installing a beta or RC version of VMware Tools and you see a warning that a package or driver is not signed, click **Install Anyway** to complete the installation.

8 When prompted, reboot the virtual machine.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

(Recommended) If you upgraded VMware Tools as part of a larger, system-wide upgrade, next upgrade to the newest virtual hardware version available for the virtual machine.

Manually Install or Upgrade VMware Tools in a Linux Virtual Machine

For Linux virtual machines, you manually install or upgrade VMware Tools by using the command line.

Install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management. When you power on a virtual machine, if a new version of VMware Tools is available, you see a notification in the status bar of the guest operating system.

NOTE This procedure describes how to use the VMware Tools tar installer to install or upgrade VMware Tools. For virtual machines in a vSphere environment, you can alternatively use VMware Tools operating system specific packages (OSPs) to install and upgrade VMware Tools. With OSPs you can use the native update mechanisms of your operating system to download, install, and manage VMware Tools. For more information, see "Operating System Specific Packages for Linux Guest Operating Systems," on page 158.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

Procedure

1 Select the menu command to mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools

2 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

3 In the virtual machine, log in to the guest operating system as root and open a terminal window.

4 Run the `mount` command with no arguments to determine whether your Linux distribution automatically mounted the VMware Tools virtual CD-ROM image.

If the CD-ROM device is mounted, the CD-ROM device and its mount point are listed as something like this:

```
/dev/cdrom on /mnt/cdrom type iso9660 (ro,nosuid,nodev)
```

5 If the VMware Tools virtual CD-ROM image is not mounted, mount the CD-ROM drive.

   a If a mount point directory does not already exist, create it.

   ```
   mkdir /mnt/cdrom
   ```

   Some Linux distributions use different mount point names. For example, on some distributions the mount point is `/media/VMware Tools` rather than `/mnt/cdrom`. Modify the command to reflect the conventions that your distribution uses.

   b Mount the CD-ROM drive.

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

   Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom` or if the mount point for a CD-ROM is not `/mnt/cdrom`, modify the command to reflect the conventions that your distribution uses.

6 Change to a working directory (for example, `/tmp`).

```
cd /tmp
```

7 Delete any previous `vmware-tools-distrib` directory before you install VMware Tools.

The location of this directory depends on where you placed it during the previous installation. Often this directory is placed in `/tmp/vmware-tools-distrib`.

8 List the contents of the mount point directory and note the filename of the VMware Tools tar installer.

```
ls mount-point
```

9 Uncompress the installer.

```
tar zxpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

The value *x.x.x* is the product version number, and *yyyy* is the build number of the product release.

If you attempt to install a tar installation over an RPM installation, or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

10 If necessary, unmount the CD-ROM image.

```
umount /dev/cdrom
```

If your Linux distribution automatically mounted the CD-ROM, you do not need to unmount the image.

11 Run the installer and configure VMware Tools.

```
cd vmware-tools-distrib
./vmware-install.pl
```

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

12 Respond to the prompts by pressing Enter to accept the default values, if appropriate for your configuration.

13 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

(Recommended) If you upgraded VMware Tools as part of a larger, system-wide upgrade, next upgrade to the newest virtual hardware version available for the virtual machine.

Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine

For Solaris virtual machines, you manually install or upgrade VMware Tools by using the command line.

Install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management. When you power on a virtual machine, if a new version of VMware Tools is available, you see a notification in the status bar of the guest operating system.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

Procedure

1 Select the menu command to mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools

2 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

3 In the virtual machine, log in to the guest operating system as root and open a terminal window.

4 If the Solaris volume manager does not mount the CD-ROM under `/cdrom/vmwaretools`, restart the volume manager.

```
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
```

5 Change to a working directory (for example, `/tmp`).

```
cd /tmp
```

6 Extract VMware Tools.

```
gunzip –c /cdrom/vmwaretools/vmware–solaris–tools.tar.gz | tar xf –
```

7 Run the installer and configure VMware Tools.

```
cd vmware–tools–distrib
./vmware–install.pl
```

Usually, the `vmware–config–tools.pl` configuration file runs after the installer file finishes running.

8 Respond to the prompts by pressing Enter to accept the default values, if appropriate for your configuration.

9 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

(Recommended) If you upgraded VMware Tools as part of a larger, system-wide upgrade, next upgrade to the newest virtual hardware version available for the virtual machine.

Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine

For NetWare virtual machines, you manually install or upgrade VMware Tools by using the command line.

Install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management. When you power on a virtual machine, if a new version of VMware Tools is available, you see a notification in the status bar of the guest operating system.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

Procedure

1 Select the menu command to mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**

2 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

3 Load the CD-ROM driver so that the virtual CD-ROM device mounts the ISO image as a volume.

Operating System	Command
NetWare 6.5	`LOAD CDDVD`
NetWare 6.0 or NetWare 5.1	`LOAD CD9660.NSS`
NetWare 4.2 (not available in vSphere)	`load cdrom`

When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger Screen for NetWare 6.5 and NetWare 6.0 guest operating systems and in the Console Screen for NetWare 4.2 and 5.1 operating systems.

4 If the VMware Tools virtual disc (`netware.iso`) is attached to the virtual machine, right-click the CD-ROM icon in the status bar of the console window and select **Disconnect** to disconnect it.

What to do next

(Recommended) If you upgraded VMware Tools as part of a larger, system-wide upgrade, next upgrade to the newest virtual hardware version available for the virtual machine.

Operating System Specific Packages for Linux Guest Operating Systems

For vSphere deployments, VMware provides operating system specific packages (OSPs) as a packaging and distribution mechanism for VMware Tools. These VMware Tools OSPs are packaged using native package formats and standards such as `rpm` and `deb`.

Using OSPs provides the following benefits:

- You can use the native update mechanisms of the guest operating system to download, install, and manage VMware Tools.
- You can upgrade to the latest version of VMware Tools without having to upgrade to the latest version of vSphere.
- Because VMware Tools OSPs follow the best practices and standards of the specific Linux operating system, OSPs use standard mechanisms for determining dependencies among packages. These mechanisms allow you to audit the packages on virtual machines with or without graphics components.
- You can use standard operating system tools to examine OSPs during VMware Tools installation. This process allows you to easily determine which components to install and to verify the validity of the packaging.

IMPORTANT Use OSPs if you want to use native update mechanisms, rather than vCenter Server, to manage updates for VMware Tools. If you use an OSP, the VMware Tools status is **unmanaged** on the virtual machine **Summary** tab. The status **unmanaged** means that you cannot use vCenter Server to manage VMware Tools and you cannot use vSphere Update Manager to upgrade VMware Tools.

For more information, go to the VMware Operating System Specific Packages Web site, at http://www.vmware.com/download/packages.html.

Perform an Automatic Upgrade of VMware Tools

When you start an automatic upgrade of VMware Tools, you do not need to perform any operations in the guest operating system that is running on the virtual machine. The automatic upgrade uninstalls the previous version of VMware Tools, installs the latest version that is available for your ESXi host, and if necessary, reboots the virtual machine.

Automatic VMware Tools upgrade is not supported for virtual machines with Solaris or NetWare guest operating systems.

Prerequisites

The following requirements are for each virtual machine in the upgrade:

- Power on the virtual machine.
- Verify that the guest operating system is running.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

Procedure

1 Select **Automatic Tools Upgrade**.

2 (Optional) In the **Advanced Options** field, enter advanced options for the guest operating system.

Option	Description
Microsoft Windows Guest Operating Systems	Enter `/s /v "/qn" /l "Microsoft_Windows_location\filename.log"` to perform a silent upgrade of VMware Tools and create a log file in the specified location on the guest operating system.
Linux Guest Operating Systems	■ Enter `--default` to perform the default behavior. Perform a silent upgrade of VMware Tools. Install tools `bin`, `lib` and `doc` files in the default `/usr` directory. ■ Enter `--prefix=binary_location,lib_location,doc_location` to perform a silent upgrade of VMware Tools and install the binary, library, and document files in the specified locations.

3 Click **OK.**

The **VMware Tools** label on the **Summary** tab changes to **OK**.

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

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

What to do next

Upgrade the virtual machine hardware to version 8.

Upgrade VMware Tools on Multiple Virtual Machines

You can upgrade VMware Tools on multiple virtual machines by using the **Virtual Machines** tab.

Procedure

1 Start the vSphere Client and log in to the vCenter Server.

2 Select **Inventory > Hosts and Clusters**.

3 Select the host or cluster that contains the virtual machines to upgrade.

4 Click the **Virtual Machines** tab.

5 Select and power on the virtual machines to upgrade.

6 Right-click your selections, select **Guest > Install/Upgrade VMware Tools** and click **OK**.

7 For Linux guest operating systems, reboot the operating system by running the `reboot` command from a command-line prompt so that you can use the new network modules.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

(Recommended) Upgrade the virtual machine hardware to version 8. See "Upgrade Virtual Hardware on Multiple Virtual Machines," on page 162.

Configure a Virtual Machine to Upgrade VMware Tools Automatically

You can configure a virtual machine to check for and apply VMware Tools upgrades each time you power on the virtual machine.

Automatic VMware Tools upgrade is not supported for virtual machines with Solaris or NetWare guest operating systems.

Prerequisites

- Virtual machines must have a version of VMware Tools shipped with ESX 3.0.1 or later installed.
- Virtual machines must be hosted on an ESX 3.0.1 or later, and VirtualCenter must be version 2.0.1 or later.
- Virtual machines must be running a Linux or Microsoft Windows guest operating system that is supported by ESX 3.0.1 or later and VirtualCenter 2.0.1 or later.

Procedure

1 Start the vSphere Client or vSphere Web Client and log in to the vCenter Server.

2 Power off the virtual machine.

3 Right-click the virtual machine and select the menu command to edit the virtual machine settings.

VMware Product	Menu Command
vSphere Client	Edit Settings
vSphere Web Client	Configuration > Edit Settings

4 On the **Options** tab (vSphere Client) or the **VM Options** tab (vSphere Web Client), select **VMware Tools**.

5 In the **Advanced** pane, select the menu command to upgrade VMware Tools automatially.

VMware Product	Menu Command
vSphere Client	Check and upgrade Tools during power cycling
vSphere Web Client	Check and upgrade VMware Tools before each power on

6 Click **OK**.

The next time you power on the virtual machine, it checks the ESXi host for a newer version of VMware Tools. On Linux guests, if a newer version is available, it is installed and the guest operating system is restarted (if required). On Windows guests, if a newer version is available, it is installed the next time you shut down or restart the virtual machine.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

Upgrade the virtual machine hardware to version 8.

Upgrade Virtual Hardware

You can upgrade the hardware version of virtual machines to the latest version of ESXi. For virtual machines that are running on ESXi 5.x, VMware recommends that you upgrade the virtual hardware to version 8.

Consider the following points:

- When you upgrade from virtual hardware version 4 to version 8 the upgrade is reversible if you take a virtual machine backup or snapshot before performing the upgrade.

- Upgraded virtual machines cannot be powered on by an ESX 2.x host, even if relocated to a VMFS2 datastore.
- To automate this process, consider using Update Manager for virtual machine upgrades. See the *Installing and Administering VMware vSphere Update Manager* documentation. Update Manager takes automatic snapshots before performing virtual machine upgrades. See "Perform an Orchestrated Upgrade of Virtual Machines with vSphere Update Manager," on page 147.
- When you upgrade virtual hardware, no downtime is required for vCenter Server or ESX/ESXi hosts. For virtual machines, the only significant downtime is the time to reboot the guest operating systems.

Prerequisites

- Create a backup or snapshot of the virtual machine. See the *vSphere Virtual Machine Administration* documentation.
- Upgrade VMware Tools. On Microsoft Windows virtual machines, if you upgrade the virtual hardware before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machines are stored on VMFS3, VMFS5 or NFS datastores.
- Determine the version of the virtual hardware by selecting the virtual machine from the vSphere Client or vSphere Web Client and clicking the **Summary** tab. The **VM Version** label displays the virtual hardware version.

Procedure

1 Start the vSphere Client or vSphere Web Client and log in to the vCenter Server.

2 Power off the virtual machine.

3 Right-click the virtual machine and select the menu command to upgrade virtual hardware.

VMware Product	Menu Command
vSphere Client	Upgrade Virtual Hardware
vSphere Web Client	Configuration > Upgrade Virtual Hardware

The software upgrades the virtual hardware to the latest supported version.

The **Upgrade Virtual Hardware** option appears if the virtual hardware on the virtual machine is not the latest supported version.

4 Click **Yes** to continue with the virtual hardware upgrade.

5 Power on the virtual machine.

If the virtual machine has a Microsoft Windows guest operating system, the operating system detects a new device, configures the device, and prompts you to reboot the guest operating system. If any unknown devices are recognized, the operating system prompts you to configure the device manually.

6 For Windows guest operating systems, reboot the guest operating system to make the changes take effect.

The virtual hardware version is 8 on the **VM Version** label on the virtual machine **Summary** tab.

Upgrade Virtual Hardware on Multiple Virtual Machines

You can upgrade virtual hardware on multiple virtual machines in a single operation by using the **Virtual Machines** tab.

Prerequisites

- Determine the version of the virtual hardware by selecting the virtual machine from the vSphere Client or vSphere Web Client and clicking the **Summary** tab. The **VM Version** label displays the virtual hardware version.
- Create backups or snapshots of the virtual machines. See the *vSphere Datacenter Administration* documentation.
- Upgrade VMware Tools. On Microsoft Windows virtual machines, if you upgrade the virtual hardware before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machines are stored on VMFS3, VMFS5 or NFS datastores.

Procedure

1. Start the vSphere Client or vSphere Web Client and log in to the vCenter Server.
2. Select the host or cluster that contains the virtual machines to upgrade.
3. Click the **Virtual Machines** tab.
4. Select and power off the virtual machines to upgrade.
5. Right-click your selections.
6. Select **Upgrade Virtual Hardware** and click **Yes**.
7. Power on the virtual machines.

   For Microsoft Windows guest operating systems, the operating system detects a new device, configures the device, and prompts you to reboot the guest operating system. If any unknown devices are recognized, the operating system prompts you to configure the device manually.
8. For Windows guest operating systems, reboot the guest operating system to make the changes take effect.

The virtual hardware version is 8 on the **VM Version** label on the virtual machine **Summary** tab.

Uninstall VMware Tools

Occasionally, an upgrade of VMware Tools is incomplete. You can usually solve the problem by uninstalling VMware Tools and then reinstalling.

In a vSphere deployment, if you decide to use Linux operating system specific packages to manage VMware Tools, and if you already used vSphere to install VMware Tools, you must uninstall the existing VMware Tools. For more information about Linux OSPs for VMware Tools, see "Operating System Specific Packages for Linux Guest Operating Systems," on page 158.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system.

Procedure

- Use the appropriate operating-system-specific procedure to uninstall VMware Tools.

Operating System	Action
Windows 7	Use the guest operating system's **Programs > Uninstall a program** item.
Windows Vista and Windows Server 2008	Use the guest operating system's **Programs and Features > Uninstall a program** item.
Windows XP and earlier	Use the guest operating system's **Add/Remove Programs** item.
Linux	On a Linux guest operating system that has VMware Tools installed by using an RPM installer, enter the following command in a terminal window: **`rpm –e VMwareTools`**
Linux, Solaris, FreeBSD, NetWare	Log in as root and enter the following command in a terminal window: **`vmware-uninstall-tools.pl`**
Mac OS X Server	Use the **Uninstall VMware Tools** application, found in `/Library/Application Support/VMware Tools`.

What to do next

Reinstall VMware Tools.

8 Example Upgrade Scenarios

Upgrade scenarios for vSphere 4.1 include cases with and without clustered hosts, hosts that you upgrade on the same machine on which they are currently running (in-place upgrades), and hosts that you upgrade using different machines (migration upgrades).

This chapter includes the following topics:

- "Upgrading Environments with Host Clusters," on page 165
- "Upgrading Environments Without Host Clusters," on page 166
- "Moving Virtual Machines Using vMotion During an Upgrade," on page 167
- "Moving Powered Off or Suspended Virtual Machines During an Upgrade with vCenter Server," on page 168
- "Upgrading to vCenter Server on a New Machine," on page 169
- "Migrating ESX 4.x or ESXi 4.x Hosts to ESXi 5.0 in a PXE-Booted Auto Deploy Installation," on page 170
- "Upgrading vSphere Components Separately in a VMware View Environment," on page 171

Upgrading Environments with Host Clusters

This example scenario shows how you can use vSphere Update Manager to simplify the host and virtual machine upgrade process and minimize downtime in environments that include host clusters.

For this scenario, verify the following details about your vSphere environment.

- You must have VirtualCenter 2.5 Update 6 or later or vCenter Server 4.x.
- You must have vSphere Update Manager.
- All your hosts must be ESX 4.x/ESXi 4.x or later.
- If your environment has vCenter Guided Consolidation, uninstall it before upgrading.

The following list of tasks provides a high-level overview of the upgrade process.

1 Run the vCenter Host Agent Pre-Upgrade Checker.

2 Upgrade vCenter Server 2.5 Update 6 or higher or vCenter Server 4.x to vCenter Server 5.0.

   a Make sure your database is compatible with vCenter Server 5.0. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

   b Make sure that you have the required permissions to perform this procedure. See "Prerequisites for the vCenter Server Upgrade," on page 30.

c Take a full backup of the vCenter Server database. See your database documentation.

d Back up the vCenter Server SSL certificates.

The downtime required for this upgrade is based on the amount of data in the database. During this time, you cannot perform provisioning operations, such as cloning or creating virtual machines.

After the upgrade, the hosts are automatically connected to vCenter Server 5.0 if you select that option during the upgrade process. vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) clusters are automatically reconfigured. (Check to ensure that the automatic reconfiguration is successful. In some cases, you might need to reconfigure the clusters manually.)

vCenter Server 5.0 is supported only on 64-bit systems. The upgrade method you use depends on what version of VirtualCenter or vCenter Server you are upgrading and on what system it is currently installed. For a detailed description of the upgrade procedure, see "Preparing for the Upgrade to vCenter Server," on page 27 and Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.

3 Install the vSphere Client.

You can install the vSphere Client on the same machine with your previous version of the vSphere Client. You must have the previous version of the vSphere Client to connect to previous versions of vCenter Server and ESX/ESXi.

For a detailed description of the procedure, see "Upgrade the vSphere Client," on page 61.

4 Upgrade vSphere Update Manager to vSphere Update Manager 5.0.

5 Use Update Manager to upgrade ESX 4.x/ESXi 4.x or higher hosts to ESXi 5.0.

Update Manager puts the host into maintenance mode before upgrading the host. The downtime for the procedure depends on the network speed and the server boot time.

For a detailed description of the procedure, see the *Installing and Administering VMware vSphere Update Manager* documentation.

6 Use Update Manager to upgrade your virtual machines. Update Manager ensures that the VMware Tools upgrade and the virtual hardware upgrade happen in the correct order to prevent loss of your network connectivity. Update Manager also performs automatic backups of your virtual machines in case you need to roll back after the upgrade. You can upgrade hosts in clusters without powering off the virtual machines if Distributed Resource Scheduler is available for the cluster.

7 Upgrade your product licenses:

a Either your new license keys are sent to you in email, or you get them using the license portal.

b Apply the new license keys to your assets using vCenter Server.

8 Use the vSphere Client to upgrade to VMFS5.

See the information on upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Upgrading Environments Without Host Clusters

If you have standalone ESX 4.x/ESXi 4.x hosts, you can upgrade your hosts and the vSphere Client to upgrade your virtual machines. This scenario provides a high-level overview of the upgrade process when you do not have host clusters and you do not have vSphere Update Manager.

This scenario applies to your environment whether or not you have vCenter Server.

Verify the following details about your vSphere environment.

- All your hosts must be ESX 4.x/ESXi 4.x or higher.

- If your environment has vCenter Guided Consolidation, uninstall it before upgrading.

1 Run the vCenter Host Agent Pre-Upgrade Checker.

See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 36.

2 If you have vCenter Server, upgrade to vCenter Server 5.0.

See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.

The downtime required for this upgrade is based on the amount of data in the database. During this time, you cannot perform provisioning operations, such as cloning or creating virtual machines.

After the upgrade, the hosts are automatically connected to vCenter Server 5.0 if you select that option during the upgrade process.

3 Install or upgrade the vSphere Client to version 5.0. See "Upgrade the vSphere Client," on page 61

You can install the vSphere Client on the same machine with your previous versions of the vSphere Client. You must have the previous versions of the vSphere Client to connect to previous versions of vCenter Server and ESX/ESXi.

4 For all hosts, perform an interactive upgrade using an ESXi ISO installer image stored on a CD, DVD, or USB flash drive to upgrade ESX 4.x/ESXi 4.x. See Chapter 6, "Upgrading and Migrating Your Hosts," on page 75 and "Upgrade or Migrate Hosts Interactively," on page 110.

This procedure involves putting the host into maintenance mode before you upgrade the host. The downtime for the procedure depends on the network speed and the server boot time.

In case of upgrade failure, the process does not support rollback to the previous release.

5 Upgrade your virtual machines. See Chapter 7, "Upgrading Virtual Machines," on page 143.

6 Get your license key either in email or by using the license portal.

7 Apply the new license keys to your assets using the vSphere Client..

8 Use the vSphere Client to upgrade your datastore to VMFS5.

See information about upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Moving Virtual Machines Using vMotion During an Upgrade

This scenario is a migration upgrade. The migration upgrade is a managed transition rather than a strict upgrade. By using vMotion to move virtual machines directly from one production host to another production host, you minimize downtime of the virtual machines.

The following example provides a high-level overview of the upgrade process in an environment with ESX 3.5/ESXi 3.5 or higher and vCenter Server 5.0, using vMotion to migrate your running virtual machines to ESXi 5.0. The hosts in your environment must be licensed for and able to use vMotion.

You can perform a migration upgrade without vMotion. The only difference is the amount of downtime for the virtual machines.

A migration upgrade calls for sufficient resources to run the production environment partly on older hosts and partly on upgraded hosts. Any required redundancies and safeguards must be available on both upgraded and non-upgraded infrastructure during the transition.

Prerequisites

- Verify that one or more machines meets ESXi 5.0 requirements.
- Verify that empty host storage is sufficient to hold a portion of your production virtual machines. Ideally, the storage is large enough to hold all of the migrated virtual machines. A larger capacity for virtual machines on this extra storage means fewer operations are required before all your virtual machines are migrated.

- If your environment has vCenter Guided Consolidation, uninstall it.
- Run the vCenter Host Agent Pre-Upgrade Checker. See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 36.
- Upgrade VirtualCenter 2.5 Update 6 or higher or vCenter Server 4.0 to vCenter Server 5.0. See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.

  The downtime required for this upgrade is based on the amount of data in the database. During this time, you cannot perform provisioning operations, such as cloning or creating virtual machines.
- Install the version 5.0 vSphere Client. See "Upgrade the vSphere Client," on page 61.
- If your environment has vSphere Update Manager, upgrade it to the latest version. See Chapter 5, "Upgrading Update Manager," on page 71.

Procedure

1. Use vMotion to move the virtual machines from the ESX 3.5/ESXi 3.5 or higher host.
2. Upgrade the host to ESXi 5.0, or perform a fresh installation of ESXi 5.0.
3. Add the ESXi 5.0 host to vCenter Server.
4. Use vMotion to move the virtual machines that you removed from the ESX 3.5/ESXi 3.5 or higher host before the upgrade.

   For vMotion to work, the hosts must be managed by the same vCenter Server instance.

What to do next

For all hosts and virtual machines in the migration upgrade, take the following actions.

- Upgrade your virtual machines. See Chapter 7, "Upgrading Virtual Machines," on page 143.
- Upgrade your product licenses:
  a. Get your new license keys by email, or by using the license portal.
  b. Apply the new license keys to your assets using the vSphere Client (or vCenter Server if you have it).
- Use the vSphere Client to upgrade the host datastore to VMFS5.

  See the information about upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Moving Powered Off or Suspended Virtual Machines During an Upgrade with vCenter Server

In a cold migration upgrade, you power off or suspend the virtual machines that you move to a new host. When you use cold migration to move virtual machines, more downtime is required for the virtual machines.

This scenario assumes that the hosts do not have vMotion capabilities.

Upgrades using cold migrations are useful for situations that require a multistep upgrade, such as upgrades from versions lower than ESX 4.x. Such upgrades require upgrading to ESX 4.x and then upgrading to ESXi 5.0.

Prerequisites

- Verify that one or more machines meets ESXi 5.0 requirements.
- Verify that empty host storage is sufficient to hold a portion of your production virtual machines. Ideally, the storage is large enough to hold all of the migrated virtual machines. A larger capacity for virtual machines on this extra storage means fewer operations are required before all your virtual machines are migrated.

- If your environment has vCenter Guided Consolidation, uninstall it before upgrading.
- Run the vCenter Host Agent Pre-Upgrade Checker. See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 36.
- Upgrade VirtualCenter 2.5 Update 6 or higher or vCenter Server 4.0 to vCenter Server 5.0. See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.
- Install the version 5.0 vSphere Client. See "Upgrade the vSphere Client," on page 61.
- If your environment has vCenter Update Manager, upgrade it to the latest version.

Procedure

1 Add the ESXi 5.0 host to vCenter Server 5.0.

2 Add the ESX 4.x/ESXi 4.x hosts to vCenter Server 5.0.

3 Power off or suspend the virtual machines on the ESX 4.x/ESXi 4.x hosts.

4 Move the virtual machines to the ESXi 5.0 host.

What to do next

For all hosts and virtual machines in the migration upgrade, take the following actions.

- Upgrade your virtual machines. See Chapter 7, "Upgrading Virtual Machines," on page 143.
- Upgrade your product licenses:
  a Get your new license keys by email, or by using the license portal.
  b Apply the new license keys to your assets using the vSphere Client (or vCenter Server if you have it).

Upgrading to vCenter Server on a New Machine

The vCenter Server installation media include a data migration tool that you can use to migrate configuration information such as port settings, SSL certificates, and license information from the source vCenter Server machine to the new machine. Instead of performing an in-place upgrade to vCenter Server, you might want to use a different machine for your upgrade. If you are upgrading from a version of VirtualCenter or vCenter Server installed on a 32-bit platform, you must use this method to upgrade to a 64-bit platform.

You can also use the data migration tool to migrate a SQL Server Express database that is installed by the vCenter Server installer on the same machine as vCenter Server. If you use another database that is installed on the vCenter Server machine, you must back up and move the database manually to the new machine. If the database is installed on a different machine from vCenter Server, you can leave the database in place and create a DSN on the destination machine to connect to it.

If VMware vSphere Update Manager or vCenter Orchestrator is installed on the same machine as vCenter Server, you can use the data migration tool to migrate configuration data for these products. You can also use the tool to migrate the Update Manager database if it is a SQL Server Express database installed on the same machine as Update Manager and vCenter Server. You cannot use the data migration tool to migrate the vCenter Orchestrator database. See *Installing and Configuring VMware vCenter Orchestrator* for information about upgrading these products.

The following process shows the upgrade path.

1 If you are not using a SQL Server Express database installed on the same machine as vCenter Server, create a backup of the database.

2 Run the `backup.bat` script of the data migration tool on the source machine to create a backup of the vCenter Server configuration.

3 Copy the configuration data to the destination machine.

See "Back Up VirtualCenter or vCenter Server Configuration with the Data Migration Tool," on page 50

4 If you are not using a SQL Server Express database installed on the same machine as vCenter Server, perform one of the following actions to move the database:

- Restore the database on the destination machine.
- Detach the database on the source machine, copy the database files to the destination machine, and attach the database on the destination machine.

5 Run the `install.bat` script on the destination machine.

This script launches the vCenter Server installer and installs vCenter Server with the configuration settings backed up by the `backup.bat` script.

For information about this process, see"Upgrade to vCenter Server on a Different Machine and Upgrade the Database," on page 43

Migrating ESX 4.x or ESXi 4.x Hosts to ESXi 5.0 in a PXE-Booted Auto Deploy Installation

This high-level overview describes the process for migrating an ESX/ESXi 4.x host to an ESXi 5.0 installation that is deployed by using vSphere Auto Deploy.

This scenario assumes the following details about your vSphere environment.

- The hosts that you are migrating are managed by a vCenter Server running VirtualCenter 2.5 Update 6 or later or vCenter Server 4.x.
- All hosts managed by that vCenter Server are running ESX/ESXi 3.5 Update 5 or ESX/ESXi 4.x.

The following tasks provide an overview of the migration process.

1 Create host profiles for the ESXi 4.x hosts to be migrated and attach the host profiles to the hosts.

See the *vSphere Host Profiles* documentation.

2 Upgrade the 4.x vCenter Server to version 5.0.

See Chapter 4, "Upgrading to vCenter Server 5.0," on page 27.

3 Prepare your Auto Deploy server and environment.

This preparation includes setting up the DHCP and TFTP servers that are used to PXE-boot Auto Deploy host machines and installing VMware PowerCLI.

See the information about preparing for vSphere Auto Deploy in the *vSphere Installation and Setup* documentation.

4 Apply an image profile for an ESXI 5.0 host that is deployed by using the Auto Deploy PowerCLI commands.

See the information about Auto Deploy in the *vSphere Installation and Setup* documentation.

5 Use vSphere vMotion to evacuate all virtual machines from the hosts to be migrated, and place the hosts in maintenance mode.

See the *vCenter Server and Host Management* documentation.

6 Reboot the hosts, enter the BIOS, and reconfigure the hosts to boot from the network.

See the information about Auto Deploy in the *vSphere Installation and Setup*. For ESXi 4.x hosts with compatible host profiles, the host configuration will be restored.

7 When one host is booted, complete any host configuration that was not migrated and take a host profile from the host.

   See the *vSphere Host Profiles* documentation.

8 Clone the host profile and attach the profile to the other migrated hosts.

   See the *vSphere Host Profiles* documentation.

9 Update the answer file of each cloned profile to provide host-specific configuration details, such as the IP configuration.

   See the *vSphere Host Profiles* documentation.

Upgrading vSphere Components Separately in a VMware View Environment

If you upgrade vSphere components separately from VMware View components, you must back up some View data and reinstall some View software.

Instead of performing an integrated upgrade of VMware View and vSphere components, you can choose to first upgrade all View components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from View components, you must perform the following additional tasks:

1 Before you upgrade vCenter Server, back up the vCenter Server database and the View Composer database.

2 Before you upgrade vCenter Server, back up the View LDAP database from a View Connection Server instance by using the `vdmexport.exe` utility.

   For instructions, see the *VMware View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.

3 If you use View Composer, after you upgrade all ESX/ESXi hosts that are managed by a particular vCenter Server instance, restart the View Composer service on that host.

4 After you upgrade VMware Tools in virtual machines that are used as View desktops, reinstall View Agent.

   Reinstalling View Agent guarantees that the drivers in the virtual machine remain compatible with the other View components.

   Step-by-step instructions for running the View Agent installer appear in the *VMware View Administration* document.

Index

Symbols

%include command **114**
%post command **114**
%pre command **114**

Numerics

64-bit
  moving to **45–47, 169**
  upgrading vCenter Server to **43**
64-bit DSN requirement **51**

A

about vSphere Upgrade **5**
acceptance levels **130**
accepteula command **114**
answer file **127**
Apply-EsxImageProfile cmdlet **126**
attaching
  baseline **104, 149**
  baseline group **104, 149**
Auto Deploy
  rebooting **125**
  reprovisioning hosts with **125**
  rule set compliance **128**
  scenario for migrating ESX/ESXi 4.x hosts to **170**
  user input **125**
Auto Deploy rules **127**
Auto Deploy,upgrading ESXi hosts with **125**
automatic upgrades, VMware Tools **160**
automatic VMware Tools upgrade **158**

B

backing up, vCenter Server configuration **50**
backup, vCenter Server database **44**
backup and restore variables (DB2) **49**
backup plans **66**
backup VirtualCenter **35**
backup.bat **50, 169**
baseline, attaching **104, 149**
baseline group, attaching **104, 149**
best practices
  updates and upgrades **75**
  vCenter Server upgrades **29**
boot command line options **113**
boot commands, entering **112**
boot prompt **113**
boot.cfg file **122**
bootloader kernel options **113**

C

CD, upgrade hosts from **110**
CD/DVD, burning the ESXi ISO image **85**
claim rule format **141**
clearpart command **114**
clients, firewall **22, 23**
cluster, configure settings **100**
cluster settings **97**
cold migration **168**
compatibility
  Database Formats for Update Manager **26**
  Operating Systems for Update Manager **26**
compliance information, viewing **105, 150**
computer name
  Oracle **35**
  SQL Server **35**
configuring
  cluster settings **100**
  host settings **99**
configuring ports **22, 23**
Connect-VIServer cmdlet **126, 127**
Copy-DeployRule cmdlet **126**
creating
  host baseline group **103**
  virtual appliance upgrade baseline **147**
  virtual machine and virtual appliance baseline group **148**

D

data migration tool
  back up **50**
  restoring **51, 52, 54**
data source name **51**
database
  backup **44**
  backup and restore (DB2) **47**
  backup and restore (Oracle) **47**
  backup and restore (SQL) **45**
  detach and attach (SQL) **46**
database connections, number of **65**
databases, preparing **64**

datastore names and vCenter Server upgrades **38**
datastore permissions
upgrade **68**
upgrading **67**
datastores, privileges **67**
DB2 **34**
depot, software **130**
DHCP, for PXE booting the ESXi installer **91**
directory **64**
disks
local **165**
VMDK **27**
DNS load balancing solutions and datastores in vCenter Server **38**
DNS Requirements **24**
download the vCenter Server installer **38**
downtime
during virtual hardware upgrade **152**
during VMware Tools upgrade **152**
vCenter Server **38**
DPM **97**
DRAC **25**
DRS **97**
dry run for esxcli installation or upgrade **138**
dryrun command **114**
DSN, 64-bit requirement **51**
DVD, upgrade hosts from **110**

E

ESX, upgrading **96**
ESX and ESXi 3.5 hosts, upgrade before vCenter Server upgrade **40**
ESX upgrade, preparation **75**
esxcli, upgrading hosts **129**
esxcli installation or upgrade, dry run **138**
esxcli reboot image **138**
ESXi
system requirements **13**
upgrading **96**
ESXi images, importing **102**
ESXi installation script, about **114**
ESXi ISO image, burning on a CD/DVD **85**
ESXi upgrade, preparation **75**
ESXi upgrade options **82**
ESXi, convert to evaluation mode **142**
esxupdate **96**
evaluation mode **141**

F

files affected by upgrade **76**
firewall **22, 23**
firewall configuration, changes after upgrade **79**
FT **97**
FTP **89**

G

global data **64**
gPXE **89**
groups, requirements **64**
guest operating systems **16**

H

HA **97**
hardware requirements
ESXi **13**
vCenter Server **17**
vCenter Server Appliance **17**
hardware requirements,ESXi **15**
host, maintenance mode **133**
host acceptance level, display **139**
host and update acceptance levels,matching **131**
host baseline group, creating **103**
host profiles, assign with Auto Deploy **127**
host settings **97**
host upgrade **96**
host upgrade options, about **82**
host, update with third-party ZIP files **136**
hosts
manually scanning **104**
remediation against baseline groups **108**
remediation against upgrade baseline **105**
remediation failure response **99**
reprovisioning with Auto Deploy **125**
hosts firewall **22, 23**
hosts, adding third party extensions **137**
hosts, upgrading **75**

I

IBM DB2, requirements **33**
IDE disks **13, 15**
IIS, conflict with vCenter Server over port 80 **24**
ILO **25**
image profile
defined **130**
display **139**
image profiles, maintenance mode for installing or updating **132**
image profiles, update host with **134**
import, ESXi image **102**
in-place upgrades **38, 165**
include command **114**
install, VMware Tools **143, 144**
install command **114**
install.bat **52, 54**
installation precheck script, errors **139**

installation script
customized in ISO image **88**
path to **114**
supported locations **114**
installing, VirtualCenter Server **64**
installing ESXi, scripted **111**
installing the vSphere Client **61**
installing VMware Tools
Linux (tar installer) **154**
Microsoft Windows **153**
NetWare (tar installer) **157**
Solaris (tar installer) **156**
installorupgrade command **114**
IP addresses **85**
ISO image, with custom installation script **88**

J

JVM heap settings, recommended for vCenter Virtual Appliance **17**

K

keyboard command **114**
kickstart commands **121**

L

LDAP **64**
license server
managing legacy hosts **62**
migrating **57**
license, reapplying after upgrade **142**
licensed mode **141**
licensing, vCenter Server **60**
Linked Mode
and databases **63, 64**
and permissions **63, 64**
requirements **64**
Linked Mode group **60, 64**
Linux guest, VMware Tools installation or upgrade (tar installer) **154**
Linux operating system specific packages for VMware Tools **158, 162**
log files **141**
logging, providing space for **21**
LUN masking **141**

M

MAC address **92**
maintenance mode, host **133**
media options, ESXi installer, supported **85**
memory, ESXi requirements **13, 15**
Microsoft .NET Framework **21**
Microsoft SQL Server, requirements **33**
Microsoft Windows guest operating system, VMware Tools installation or upgrade **153**
migrating, license server **57**
migrating ESX 4.x files to ESXi 5.0 **76**
migration upgrade **38, 167, 168**

N

NetWare guest operating system, VMware Tools installation or upgrade (tar installer) **157**
network command **92, 114**
network permissions
upgrade **69**
upgrading **67**
networking changes in ESXi 5.0 **79**
networks, permissions **69**
New-DeployRule cmdlet **127**

O

operating system specific packages for VMware Tools in Linux virtual machines **158, 162**
Oracle **34**
Oracle database
changing the computer name **35**
requirements **33**
Oracle JDBC Driver **60**
orchestrated host upgrades **96**
orchestrated upgrade
of hosts **98**
of virtual machines **147**
OSPs for installing VMWare Tools in Linux virtual machines **158, 162**

P

paranoid command **114**
part command **114**
partition command **114**
Partitioning, changes from ESX 4.x and ESXi 4.x to ESXi 5.0 **80**
partitioning, fresh ESXi 5.0 installations **81**
partitioning, upgraded ESXi 5.0 hosts **81**
permissions, networks **69**
plug-ins, updating with new machine name **56**
port 80 conflict between vCenter Server and IIS **24**
ports
443 **30**
80 **30**
configuring **22, 23**
firewall **22, 23**
ports used by vCenter Server **22**
ports used by vCenter Server Appliance **23**

postupgrade considerations **141**
postupgrade considerations for vCenter Server **60**
pre-upgrade checker, for vCenter Agent **36**
privileges, datastores **67**
process for upgrading **165**
PXE, configuration files **92**
PXE boot ESXi installer using PXELINUX, setup procedure **92, 94, 95**
PXE booted ESXi hosts, enable remediation **101**
PXELINUX
  boot ESXi installer using **92, 95**
  boot ESXi installler using **94**

R

reboot image **138**
remediation
  of hosts **105, 108**
  of virtual appliances **151**
  of virtual machines **151**
remote management applications **96**
Repair-DeployRulesetCompliance cmdlet **128**
requirements for vSphere Client **21**
requirements for vSphere Web Client **21**
resource pool settings affected by upgrade **79**
restoring, vCenter Server configuration **51, 52, 54**
restoring VirtualCenter 2.x **66**
ROM image **89**
rootpw command **114**
RSA **25**
rule set compliance **128**

S

SAS disks **13, 15**
SATA disks **13, 15**
scanning
  hosts **104**
  virtual appliance **150**
  virtual machine **150**
scenarios **27, 165**
script, for installing ESXi **114**
scripted installation, differences from ESXi 4.x **121**
scripted upgrade of ESXi, by PXE Booting **124**
scripted upgrade of ESXi, from a USB flash drive **123**
scripted upgrade of ESXi,from a CD or DVD **122**
SCSI **13, 15**
Service Console, removed in ESXi 5.0 **11**
Service Console port group **80**
services, VMware Tools **143, 144**
settings affected by upgrade **76**
software depot, defined **130**
Solaris guest operating system, VMware Tools installation or upgrade (tar installer) **156**
specifications
  ESXi hardware requirements **13, 15**
  performance recommendations **13, 15**
SQL compatibility mode **39, 40**
SQL Server, changing the computer name **35**
SQL Server Express database, back up **50**
SSH configuration, affected by upgrade **79**
SSL certificates **60, 169**
static IP addresses **85**
supported database formats **26**
system requirements, vCenter Server database **33**

T

tar installer **154**
TCP/IP **30**
Test-DeployRuleSetCompliance cmdlet **128**
TFTP **89**
tftp-hpa **89**
tftpd32 **89**
Tomcat service, vCenter Server upgrade failure **60**

U

uninstalling VMware Tools **162**
Update Manager
  hardware requirements **25**
  supported Operating Systems **26**
  upgrading **71**
updated information **7**
upgrade
  in place **165**
  migration **167, 168**
  process **9, 165**
  virtual machines **147**
  VMware Tools **143, 144**
upgrade command **114**
upgrade hosts **105**
upgrade hosts interactively **110**
upgrade on new hardware, vCenter Server **34**
upgrade precheck script, errors **139**
upgrade scenario without host clusters **166**
upgrade scenarios **27, 165**
upgrade support for ESXi 5.0.x **84**
upgrade virtual hardware **160**
upgrade VMware Tools, automatic **158**
upgrades, best practices **75**

upgrading
datastore permissions **67**
network permissions **67**
stage 1 **27, 38**
stage 4 **144**
Update Manager **71**
Update Manager Client **73**
Update Manager server **71**
vCenter Server **27**
vCenter Server database **30**
vCenter Server on a different machine **43**
virtual machine hardware **146**
vSphere Client **27**
upgrading ESXi, scripted **111**
upgrading hosts **75**
upgrading hosts using esxcli **129**
upgrading virtual hardware **162**
upgrading VMware Tools
Linux (tar installer) **154**
Microsoft Windows **153**
NetWare (tar installer) **157**
process overview **144**
Solaris (tar installer) **156**
USB drive, upgrade hosts from **110**
USB, bootable ESXi installation **86**
USB, ESXi installation script **87**
use cases **165**
user input for Auto Deploy **127**
user input for Auto Deploy hosts **125**
utilities, VMware Tools **143, 144**

V

vCenter Host Agent, pre-upgrade checker **36**
vCenter Host Agent Pre-Upgrade Checker **36**
vCenter Server
database **44**
downloading the installer **38**
hardware requirements **17**
joining a group **64**
ports **22**
postupgrade considerations **60**
postupgrade tasks **65**
requirements for joining a group **64**
software requirements **20**
system requirements **13**
upgrade preparation tasks **171**
upgrading **27**
vCenter Server Appliance
ports **23**
See also VMware vCenter Server Appliance
vCenter Server Appliance,updating from a zipped update bundle **59**
vCenter Server Appliance,updating from the CD-ROM drive **60**
vCenter Server Appliance,updating from the VMware.com Repository **58**
vCenter Server Appliance,upgrading **58**
vCenter Server downtime **38**
vCenter Server upgrade, prerequisites **27**
vCenter Server upgrade fails, Tomcat service **60**
vCenter Server upgrades, best practices **29**
vCenter Server upgrades and datastore names **38**
vCenter upgrade **27**
vCenter Virtual Appliance, JVM heap settings **17**
VI Client **61**
VIB, defined **130**
VIBs
acceptance levels **130**
migrating in upgrade **83**
VIBs, maintenance mode for installing or updating **132**
VIBs, removing from host **136**
VIBs, update host with **133**
View Agent, upgrade procedure **171**
viewing, compliance information **105, 150**
vihostupdate **96**
virtual appliance
manually scan **150**
scanning **150**
virtual appliance remediation **151**
virtual appliance upgrade baseline, creating **147**
virtual CD **96**
Virtual Center, upgrading to vCenter Server **41**
virtual hardware, upgrading **143, 162**
virtual hardware upgrade, downtime **152**
virtual machine
manually scan **150**
scanning **150**
virtual machine and virtual appliance baseline group, creating **148**
virtual machine hardware, upgrading **146**
virtual machine hardware version **146**
virtual machine remediation **151**
virtual machines
downtime during upgrade **152**
hardware versions **146**
RAM requirements **13, 15**
upgrade **147**
upgrading hardware version **146**
virtual machines upgrade **145**
VirtualCenter, backup **35**
VirtualCenter 2.x, restoring after upgrade **66**
vmaccepteula command **114**
vMotion **167**

VMware Tools
automate upgrades **159, 160**
install and upgrade **143, 144**
upgrade procedure **171**
VMware Tools installation
Linux (tar installer) **154**
Microsoft Windows **153**
NetWare (tar installer) **157**
Solaris (tar installer) **156**
VMware Tools upgrade
downtime **152**
Linux (tar installer) **154**
Microsoft Windows **153**
NetWare (tar installer) **157**
process **144**
Solaris (tar installer) **156**
VMware Tools upgrade, automatic **158**
VMware vCenter Server Appliance
hardware requirements **17**
software requirements **20**
vpxa, *See* vCenter Agent
vSphere, upgrading components separately **171**
vSphere 5.0, changes from vSphere 4.x.x **11**
vSphere Authentication Proxy, IIS installation causes port 80 conflict **24**
vSphere Client
downloading **61**
hardware requirements **17**
installing **61**
requirements **21**
vSphere Update Manager, orchestrated upgrade of virtual machines **147**
vSphere Web Client
hardware requirements **17**
requirements **21**