vSphere Installation and Setup

vSphere 5.1

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-000805-02

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About vSphere Installation and Setup

vSphere Installation and Setup describes how to install new configurations of VMware® vCenter Server and ESXi.

Intended Audience

vSphere Installation and Setup is intended for anyone who needs to install and set up vCenter Server and ESXi 5.1.

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

Updated Information

This *vSphere Installation and Setup* is updated with each release of the product or when necessary.

This table provides the update history of *vSphere Installation and Setup*.

Revision	Description
EN-000805-02	■ Documented additional required ports for vCenter Single Sign-On: "Required Ports for vCenter Server," on page 39. ■ Documented an additional requirement for autodiscovery of Active Directory domains during vCenter Single Sign On installation: "Adding Active Directory and OpenLDAP Domains to vCenter Server 5.1," on page 228. ■ Updated the following topics to remove procedures and privileges no longer applicable in vSphere 5.1 and to add procedures and privileges required for vSphere 5.1: ■ "(Optional) Use a Script to Create Microsoft SQL Server Database Objects Manually," on page 209. ■ "(Optional) Use a Script to Create the DB2 Database Schema," on page 200. ■ "(Optional) Use a Script to Create the Oracle Database Schema," on page 216.
EN-000805-01	■ Changed command in Step 2 of Creating Image Profiles from Scratch Workflow. "Creating Image Profiles from Scratch Workflow," on page 164. ■ Updated Table Table 10-1. ■ Updated topic: "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221. ■ Updated entry for Oracle in Table: Table 9-1. ■ Updated and added topics to provide more information about installing vCenter Single Sign-On in basic, high availability, and multisite modes: "Separately Install vCenter Single Sign-On," on page 251 and subtopics. ■ Updated topic: "Install vCenter Single Sign-On as Part of a vCenter Server Simple Install," on page 247. ■ Added topic: "Confirm Active Directory Domains for vCenter Server Administrators," on page 265. ■ Added topic: "(Optional) Replicate Data Between Multisite Single Sign-On Instances in a New vCenter Server Deployment," on page 267. ■ Updated topic: "Install vCenter Server in a Separate Installation," on page 268. ■ Updated topic: "vCenter Single Sign-On Deployment Modes," on page 225. ■ Updated topic: "Adding Active Directory and OpenLDAP Domains to vCenter Server 5.1," on page 228. ■ Updated topic: "How vCenter Single Sign-On Deployment Scenarios Affect Log In Behavior," on page 229 and subtopics. ■ Updated topic: "Required vCenter Single Sign-On Database Users," on page 243. ■ Updated topic "Required vCenter Single Sign-On Database Users," on page 243. ■ Added topic: "vCenter Single Sign-On Installation Fails," on page 271. ■ Added topic: "vCenter Single Sign-On Fails at Start Up or During Initialization," on page 271. ■ Added topic: "If Autodiscovery Fails During Single Sign-On Installation Manually Add Active Directory Domains," on page 272. ■ Updated the following topics to clarify that version 5.0.x vCenter Servers can only be linked with other 5.0.x vCenter Servers, and 5.1.x vCenter Servers can only be linked with other 5.1.x vCenter Servers: "Linked Mode Considerations for vCenter Server," on page 294, "Linked Mode Prerequisites for vCenter Server," on page 294, and "Join a Linked Mode Group After Installation," on page 296.
EN-000805-00	Initial release.

Introduction to vSphere Installation and Setup 1

vSphere 5.1 provides various options for installation and setup. To ensure a successful vSphere deployment, understand the installation and setup options, and the sequence of tasks required.

You have several options for installing and setting up ESXi, for managing vSphere with vCenter Server, the vSphere Client, and the vSphere Web Client, and for the database setup that you use with vCenter Server.

This chapter includes the following topics:

How vSphere 5.x Differs from vSphere 4.x

vSphere 5.x 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.x, see the release notes for version 5.x releases.

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.x, 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 Chapter 5, "Installing ESXi Using vSphere Auto Deploy," on page 65 and Chapter 6, "Using vSphere ESXi Image Builder CLI," on page 145.

Changes in the ESXi installation and upgrade process

ESXi 5.x uses a single installer wizard for fresh installations and upgrades. ESXi 5.x 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.x. You cannot upgrade or migrate from earlier ESX or ESXi versions to ESXi 5.x by using any command-line utility. After you have upgraded or migrated to ESXi 5.x, you can upgrade or patch ESXi 5.x hosts using vCLI `esxcli` commands.

IMPORTANT After you upgrade or migrate your host to ESXi 5.x, 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.

If you are upgrading an existing ESX or ESXi host, see the *vSphere Upgrade* documentation.

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.x 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.x hosts use VMFS5, an updated version of the VMware File System for vSphere 5.x. Unlike earlier versions, ESXi 5.x 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.

NOTE Partitioning for hosts that are upgraded to ESXi 5.x differs significantly from partitioning for new installations of ESXi 5.x. See the *vSphere Upgrade* documentation.

VMware vCenter Server Appliance

As an alternative to installing vCenter Server on a Windows machine, vSphere 5.x 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.

vCenter Single Sign On vSphere 5.1 introduces vCenter Single Sign On as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation. Authentication by vCenter Single Sign On makes the VMware cloud infrastructure platform more secure by allowing the vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. See "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224.

Installing ESXi on a Drive with an Existing ESX or ESXi Installation or VMFS Datastore

ESXi 5.x uses the same installer for fresh installations and upgrades or migrations. If the installer finds an existing ESX/ESXi 4.x or ESXi 5.0 installation, it provides the option to upgrade or to do a fresh installation.

See *vSphere Upgrade*.

Depending on the disk layout of your system, the ESXi installer offers a choice between preserving or overwriting the VMFS datastore during installation.

Overview of the vSphere Installation and Setup Process

vSphere is a sophisticated product with multiple components to install and set up. To ensure a successful vSphere deployment, understand the sequence of tasks required.

Installing vSphere includes the following tasks:

1. Verify that your system meets vSphere hardware and software requirements. See Chapter 2, "System Requirements," on page 29.
2. Determine the ESXi installation option to use. See "Options for Installing ESXi," on page 14.
3. Determine where you will locate and boot the ESXi installer. See "Media Options for Booting the ESXi Installer," on page 16. If you are PXE-booting the installer, verify that your network PXE infrastructure is properly set up. See "PXE Booting the ESXi Installer," on page 20.
4. Install ESXi:
   - Chapter 3, "Installing ESXi Interactively," on page 45
   - Chapter 4, "Installing, Upgrading, or Migrating Hosts Using a Script," on page 49
   - Chapter 5, "Installing ESXi Using vSphere Auto Deploy," on page 65
5. Configure ESXi boot and network settings, the direct console, and other settings. See Chapter 7, "Setting Up ESXi," on page 167.
6. Install the vSphere Client to manage your ESXi host. License your host and back up your host configuration. See Chapter 8, "After You Install and Set Up ESXi," on page 189.

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 38, "Configure Syslog on ESXi Hosts," on page 183, "Set Up Syslog from the Host Profiles Interface in the vSphere Client," on page 101, and "Install or Upgrade vSphere Syslog Collector," on page 288.

8 (Optional) Perform these tasks if you are using vCenter Server to manage your vSphere deployment:

   a Set up vCenter Server databases. See Chapter 9, "Preparing vCenter Server Databases," on page 193.

   b Install vCenter Single Sign On, Inventory Service, vCenter Server, and vCenter Server support tools. Connect to vCenter Server from the vSphere Client or the vSphere Web Client. See Chapter 11, "Installing vCenter Server," on page 245 and Chapter 12, "After You Install vCenter Server," on page 279.

   c (Optional) Create a Linked Mode Group or join vCenter Server to a Linked Mode Group. See "Creating vCenter Server Linked Mode Groups," on page 293.

Options for Installing ESXi

ESXi can be installed in several ways. To ensure the best vSphere deployment, understand the options thoroughly before beginning the installation.

ESXi installations are designed to accommodate a range of deployment sizes.

Depending on the installation method you choose, different options are available for accessing the installation media and booting the installer.

Interactive ESXi Installation

Interactive installations are recommended for small deployments of fewer than five hosts.

You boot the installer from a CD or DVD, from a bootable USB device, or by PXE booting the installer from a location on the network. You follow the prompts in the installation wizard to install ESXi to disk. See Chapter 3, "Installing ESXi Interactively," on page 45.

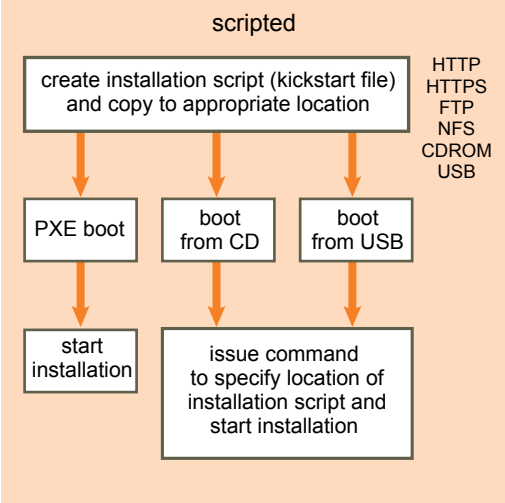
Scripted ESXi Installation

Running a script is an efficient way to deploy multiple ESXi hosts with an unattended installation.

The installation script contains the host configuration settings. You can use the script to configure multiple hosts with the same settings. See Chapter 4, "Installing, Upgrading, or Migrating Hosts Using a Script," on page 49.

The installation script must be stored in a location that the host can access by HTTP, HTTPS, FTP, NFS, CDROM, or USB. You can PXE boot the ESXi installer or boot it from a CD/DVD or USB drive.

Figure 1-1. Scripted Installation



Auto Deploy ESXi Installation

vSphere 5.1 provides several ways to install ESXi with Auto Deploy.

These topics describe Auto Deploy options for ESXi installation.

Provisioning ESXi Hosts UsingvSphere Auto Deploy

With the vSphere Auto Deploy ESXi feature, you can provision and reprovision large numbers of ESXi hosts efficiently with vCenter Server.

When you provision hosts using the Auto Deploy feature, vCenter Server loads the ESXi image directly into the host memory. Auto Deploy does not store the ESXi state on the host disk. vCenter Server makes image profiles with ESXi updates and patches available for download through an image profile, and, optionally, the host configuration through a host profile. You can create host profiles using the vSphere Client. You can create custom image profiles with ESXi Image Builder CLI. See Chapter 6, "Using vSphere ESXi Image Builder CLI," on page 145 and *vSphere Host Profiles*.

The first time you install a host with Auto Deploy, the host PXE boots and establishes contact with the Auto Deploy server, which streams the image profile and any host profile to the host. The host starts, using the image profile, and Auto Deploy assigns the host to the appropriate vCenter Server system.

When you restart the host, the Auto Deploy server continues to provision the host with the appropriate image and host profile. To provision the host with a different image profile, change the rule that specifies the image profile and perform a test and repair compliance operation. This will propagate the change to all hosts that the rule specifies. This ability to propgate changes to multiple hosts makes Auto Deploy an efficient way to provision and reprovision large numbers of hosts, and to enforce compliance to a master ESXi image.

See "Understanding vSphere Auto Deploy," on page 66.

Using vSphere Auto Deploy for Stateful Installations

In some situations, it is useful to provision hosts with Auto Deploy and to perform all subsequent boots from disk.

You can use vSphere Auto Deploy to provision an ESXi host, and set up a host profile that causes the host to store the ESXI image and configuration on the local disk, a remote disk, or a USB drive. Subsequently, the ESXi host boots from this local image. Auto Deploy no longer provisions the host. This process issimilar to performing a scripted installation. With a scripted installation, the script provisions a host and the host then boots from disk. For this case, Auto Deploy provisions a host and the host then boots from disk.

See "Using Auto Deploy for Stateless Caching and Stateful Installs," on page 90.

vSphere Auto Deploy and Stateless Caching

You can use vSphere Auto Deploy to provision an ESXi host, and set up a host profile that causes the host to store the ESXI image and configuration on the local disk, a remote disk, or a USB drive.

Subsequently, the Auto Deploy server continues to provision this host. If the Auto Deploy server is not available, the host uses the image on disk.

See "Using Auto Deploy for Stateless Caching and Stateful Installs," on page 90.

Customizing Installations with ESXi Image Builder CLI

You can use ESXi Image Builder CLI to create ESXi installation images with a customized set of updates, patches, and drivers.

ESXi Image Builder CLI is a PowerShell CLI command set that you can use to create an ESXi installation image with a customized set of ESXi updates and patches. You can also include third-party network or storage drivers that are released between vSphere releases.

You can deploy an ESXi image created with Image Builder in either of the following ways:

- By burning it to an installation DVD.
- Through vCenter Server, using the Auto Deploy feature.

See Chapter 6, "Using vSphere ESXi Image Builder CLI," on page 145 and Chapter 5, "Installing ESXi Using vSphere Auto Deploy," on page 65.

About ESXi Evaluation and Licensed Modes

After you purchase vSphere licenses, VMware provides a serial number that you use to license ESXi hosts. You can use evaluation mode to explore the entire set of features that are available for ESXi hosts, including features that are not included in the license that you have.

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.

For information about managing licensing and setting an ESXi host to evaluation mode, see the *vCenter Server and Host Management* documentation.

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 17.
- Boot from a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 17.
- PXE boot from the network. "PXE Booting the ESXi Installer," on page 20

- Boot from a remote location using a remote management application. See "Using Remote Management Applications," on page 27

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 19.

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 `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 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 50 and "About PXE Configuration Files," on page 23.

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 52 and "About the boot.cfg File," on page 61.

Prerequisites

- Linux machine.

- The ESXi ISO image `VMware-VMvisor-Installer-5.x.x-XXXXXX.x86_64.iso`,where *5.x.x* is the version of ESXi you are installing, and *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.x.x-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_cust.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.x 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.

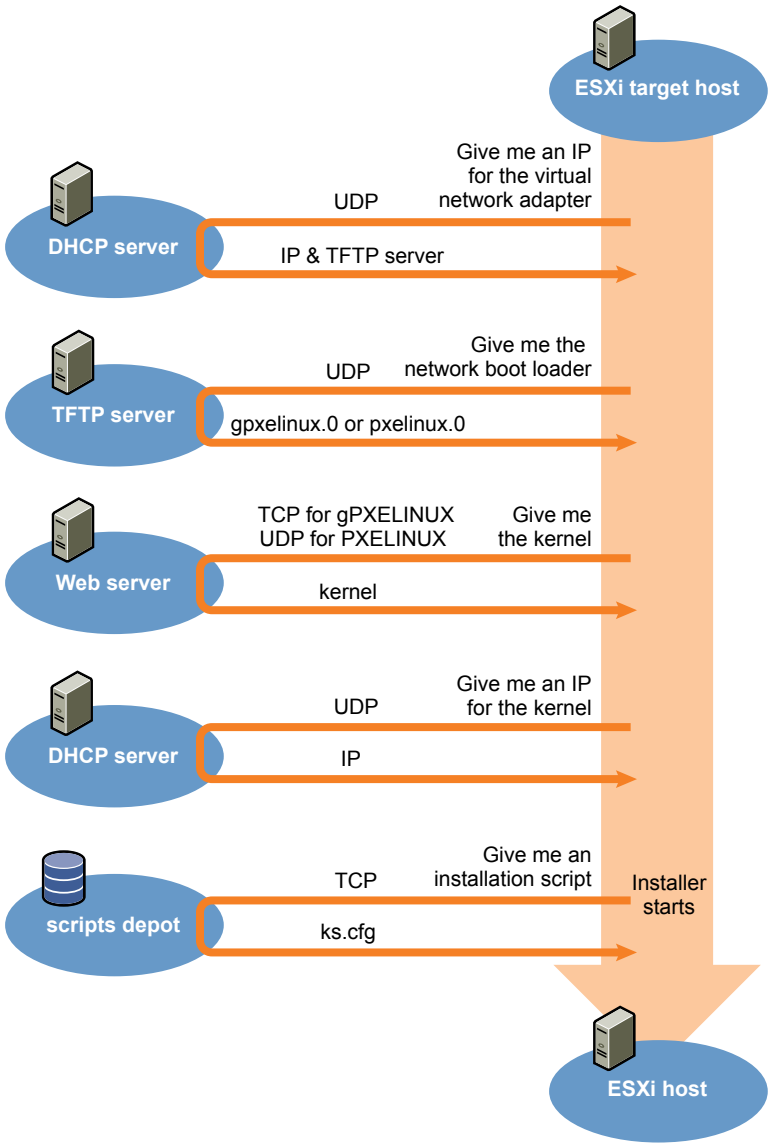
You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.

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 1-2. 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 61

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 52 and "About the boot.cfg File," on page 61

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 20.

- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 22.
- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.1. 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 52.
- 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.x.x-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.x.x-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 52 and "About the boot.cfg File," on page 61

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 20.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 22.
- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.1. 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 52.
- 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.x.x-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.x.x-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 52 and "About the boot.cfg File," on page 61

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 22.
- Server with a hardware configuration that is supported with ESXi 5.1. 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 52.

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
```

Installing and Booting ESXi with Software FCoE

You can install and boot ESXi from an FCoE LUN using VMware software FCoE adapters and network adapters with FCoE offload capabilities. Your host does not require a dedicated FCoE HBA.

See the *vSphere Storage* documentation for information about installing and booting ESXi with software FCoE.

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 43. 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.

Required Information for ESXi Installation

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

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

Table 1-1. Required Information for ESXi Installation

Information	Required or Optional	Default	Comments
Keyboard layout	Required	U.S. English	
VLAN ID	Optional	None	Range: 0 through 4094
IP address	Optional	DHCP	You can allow DHCP to configure the network during installation. After installation, you can change the network settings.
Subnet mask	Optional	Calculated based on the IP address	
Gateway	Optional	Based on the configured IP address and subnet mask	
Primary DNS	Optional	Based on the configured IP address and subnet mask	
Secondary DNS	Optional	None	
Host name	Required for static IP settings	None	vSphere Clients can use either the host name or the IP address to access the ESXi host.
Install location	Required	None	Must be at least 5GB if you install the components on a single disk.
Migrate existing ESX or ESXi settings. Preserve existing VMFS datastore.	Required if you are installing ESXi on a drive with an existing ESXi or ESX installation.	None	See "Installing ESXi on a Drive with an Existing ESX or ESXi Installation or VMFS Datastore," on page 13.
Root password	Optional	None	The root password must contain between 6 and 64 characters.

System Requirements 2

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 "Preparing for vSphere Auto Deploy," on page 75.

This chapter includes the following topics:

ESXi Hardware Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi 5.1.

Hardware and System Resources

To install and use ESXi 5.1, 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 5.1 will install and run only on servers with 64-bit x86 CPUs.
- ESXi 5.1 requires a host machine with at least two cores.
- ESXi 5.1 supports only LAHF and SAHF CPU instructions.
- ESXi 5.1 requires the NX/XD bit to be enabled for the CPU in the BIOS.

- 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. Provide at least 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 5.1 host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

ESXi 5.1 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 5.1 and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI
- USB devices. Supported for installing ESXi 5.1.

- Software Fibre Channel over Ethernet (FCoE). See "Installing and Booting ESXi with Software FCoE," on page 27.

ESXi Booting Requirements

vSphere 5.1 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 5.1 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 5.1.

Storage Requirements for ESXi 5.1 Installation

Installing ESXi 5.1 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 "Set the Scratch Partition from the vSphere Client," on page 181.

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 29.

Table 2-1. Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 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 5.1 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.

Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client

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 Single Sign On, Inventory Service and vCenter Server Hardware Requirements

You can install vCenter Single Sign On, Inventory Service, and vCenter Server on the same host machine (as with vCenter Simple Install) or on different machines. Table 2-2 and Table 2-3 list the hardware requirements for Single Sign On and Inventory Service, running on separate host machines. If you install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server on the same host machine, the Single Sign On and Inventory Service memory and disk storage requirements are in addition to the requirements for vCenter Server. See Table 2-4.

Table 2-2. Minimum Hardware Requirements for vCenter Single Sign On, Running on a Separate Host Machine from vCenter Server

vCenter Single Sign On Hardware	Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	3GB. Memory requirements might be higher if the vCenter Single Sign On database runs on the same host machine. If vCenter Single Sign On runs on the same host machine as vCenter Server, see Table 2-4.
Disk storage	2GB. Disk requirements might be higher if the vCenter Single Sign On database runs on the same host machine.
Network speed	1Gbps

Table 2-3. Minimum Hardware Requirements for vCenter Inventory Service, Running on a Separate Host Machine from vCenter Server

vCenter Inventory Service Hardware	Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	3GB. If vCenter Inventory Service runs on the same host machine as vCenter Server, see Table 2-4.
Disk storage	At least 60GB for medium- to large-sized inventories (more than 100 hosts or 1000 virtual machines). If vCenter Inventory Service runs on the same host machine as vCenter Server, see Table 2-4.
Network speed	1Gbps

Table 2-4. 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	The amount of memory needed depends on your vCenter Server configuration. ■ If vCenter Server is installed on a different host machine than vCenter Single Sign On and vCenter Inventory Service, 4GB of RAM are required. ■ If vCenter Server, vCenter Single Sign On and vCenter Inventory Service are installed on the same host machine (as with vCenter Simple Install), 10GB of RAM are required. Memory requirements are higher if the vCenter Server database or vCenter Single Sign On database runs on the same machine as vCenter Server. vCenter Server includes several Java services: VMware VirtualCenter Management Webservices (tc Server), 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 2-5.
Disk storage	The amount of disk storage needed for the vCenter Server installation depends on your vCenter Server configuration. ■ If vCenter Server is installed on a different host machine than vCenter Single Sign On and vCenter Inventory Service, 4GB are required. ■ If vCenter Server, vCenter Single Sign On and vCenter Inventory Service are installed on the same host machine (as with vCenter Simple Install), at least 40-60GB of free disk space are required after installation, depending on the size of your inventory. 100GB are recommended, to allow for future growth of your inventory. Disk storage requirements are higher if the vCenter Server database or vCenter Single Sign On database runs on the same machine as vCenter Server, depending on the size of those databases. In vCenter Server 5.x, 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.
Network speed	1Gbps

The JVM heap settings for vCenter Server depend on your inventory size. See "Configuring VMware Tomcat Server Settings in vCenter Server 5.1," on page 300.

Table 2-5. JVM Heap Settings for vCenter Server

vCenter Server Inventory	VMware VirtualCenter Management Webservices (tc Server)	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	1GB	3GB	512MB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	2GB	6GB	1GB
Large inventory (More than 400 hosts or 4000 virtual machines)	3GB	12GB	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 2-6. Hardware Requirements for VMware vCenter Server Appliance

VMware vCenter Server Appliance Hardware	Requirement
Disk storage on the host machine	The vCenter Server Appliance requires at least 7GB of disk space, and is limited to a maximum size of 80GB. The vCenter Server Appliance can be deployed with thin-provisioned virtual disks that can grow to the maximum size of 80GB. If the host machine does not have enough free disk space to accommodate the growth of the vCenter Server Appliance virtual disks, vCenter Server might cease operation, and you will not be able to manage your vSphere environment.
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 16GB. ■ Large inventory (More than 400 hosts or 4000 virtual machines): at least 24GB.

Table 2-7. JVM Heap Settings for VMware vCenter Server Appliance

vCenter Server Appliance Inventory	VMware VirtualCenter Management Webservices (tc Server)	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	1GB	3GB	512MB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	2GB	6GB	1GB
Large inventory (More than 400 hosts or 4000 virtual machines)	3GB	12GB	2GB

See "Configuring VMware Tomcat Server Settings in vCenter Server 5.1," on page 300.

vSphere Client Hardware Requirements and Recommendations

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

Table 2-8. 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 2-9. 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 2-10. 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 2-11. 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 2-12. 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
Disk Storage	At least 2GB free disk space
Networking	Gigabit connection recommended

vCenter Server Software Requirements

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

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

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

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

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

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.

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 version 5.1 of the vSphere Web Client:

- Microsoft Internet Explorer 7, 8, and 9.
- Mozilla Firefox 3.6 and later.
- Google Chrome 14 and later.

The vSphere Web Client requires the Adobe Flash Player version 11.1.0 or later to be installed with the appropriate plug-in for your browser.

Providing Sufficient Space for System Logging

ESXi 5.x 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.x autoconfigures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 2-13. 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 a remote log server, see "Configure Syslog on ESXi Hosts," on page 183, "Set Up Syslog from the Host Profiles Interface in the vSphere Client," on page 101, and "Install or Upgrade vSphere Syslog Collector," on page 288.

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 40.

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 2-14. 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 41.
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.

Table 2-14. Ports Required for Communication Between Components (Continued)

Port	Description
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
6501	Auto Deploy service
6502	Auto Deploy management
7005	vCenter Single Sign On
7009	vCenter Single Sign On
7080	vCenter Single Sign On
7444	vCenter Single Sign On HTTPS
9443	vSphere Web Client HTTPS
9090	vSphere Web Client HTTP
10080	vCenter Inventory Service HTTP
10443	vCenter Inventory Service HTTPS
10111	vCenter Inventory Service Management
10109	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 39.

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 2-15. 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 2-15. 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
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 39.

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 2-16. 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

Installing ESXi Interactively 3

Use the interactive installation option for small deployments of less than five hosts.

In a typical interactive installation, you boot the ESXi installer and respond to the installer prompts to install ESXi to the local host disk. The installer reformats and partitions the target disk and installs the ESXi boot image. If you have not installed ESXi on the target disk before, all data located on the drive is overwritten, including hardware vendor partitions, operating system partitions, and associated data.

NOTE To ensure that you do not lose any data, migrate the data to another machine before you install ESXi.

If you are installing ESXi on a disk that contains a previous installation of ESXi or ESX, or a VMFS datastore, the installer provides you with options for upgrading. See the *vSphere Upgrade* documentation.

This chapter includes the following topics:

Install ESXi Interactively

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

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 17
  - On a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 17.

  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 20.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- Verify that a keyboard and monitor are attached to the machine on which the ESXi software will be installed. Alternatively, use a remote management application. See "Using Remote Management Applications," on page 27.
- Consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. Note that when you disconnect network storage, any files on the disconnected disks are unavailable at installation.

Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.

- Gather the information required by the ESXi installation wizard. See "Required Information for ESXi Installation," on page 27.
- Verify that ESXi Embedded is not present on the host machine. 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 On the Select a Disk page, select the drive on which to install ESXi and press Enter.

Press F1 for information about the selected disk.

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

If the disk you selected contains data, the Confirm Disk Selection page appears.

If you are installing on a disc with a previous ESXi or ESX installation or VMFS datastore, the installer provides several choices.

IMPORTANT If you are upgrading or migrating an existing ESX/ESXi installation, see the *vSphere Upgrade* documentation. The instructions in this *vSphere Installation and Setup* documentation are for a fresh installation of ESXi.

4 Select the keyboard type for the host.

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

5 Enter the root password for the host.

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

6 Press Enter to start the installation.

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

8 Press Enter to reboot the host.

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

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

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

NOTE UEFI systems might require additional steps to set the boot device. See "Host Fails to Boot After You Install ESXi in UEFI Mode," on page 173

After the installation is complete, you can migrate existing VMFS data to the ESXi host.

You can boot a single machine from each ESXi image. Booting multiple devices from a single shared ESXi image is not supported.

What to do next

Set up basic administration and network configuration for ESXi. See Chapter 8, "After You Install and Set Up ESXi," on page 189.

Install ESXi on a Software iSCSI Disk

When you install ESXi to a software iSCSI disk, you must configure the target iSCSI qualified name (IQN).

During system boot, the system performs a Power-On Self Test (POST), and begins booting the adapters in the order specified in the system BIOS. When the boot order comes to the iSCSI Boot Firmware Table (iBFT) adapter, the adapter attempts to connect to the target, but does not boot from it. See Prerequisites.

If the connection to the iSCSI target is successful, the iSCSI boot firmware saves the iSCSI boot configuration in the iBFT. The next adapter to boot must be the ESXi installation media, either a mounted ISO image or a physical CD-ROM.

Prerequisites

- Verify that the target IQN is configured in the iBFT BIOS target parameter setting. This setting is in the option ROM of the network interface card (NIC) to be used for the iSCSI LUN. See the vendor documentation for your system.
- Disable the iBFT adapter option to boot to the iSCSI target. This action is necessary to make sure that the ESXi installer boots, rather than the iSCSI target. When you start your system, follow the prompt to log in to your iBFT adapter and disable the option to boot to the iSCSI target. See the vendor documentation for your system and iBFT adapter. After you finish the ESXi installation, you can reenable the option to boot from the LUN you install ESXi on.

Procedure

1 Start an interactive installation from the ESXi installation CD/DVD or mounted ISO image.

2 On the Select a Disk screen, select the iSCSI target you specified in the iBFT BIOS target parameter setting.

   If the target does not appear in this menu, make sure that the TCP/IP and initiator iSCSI IQN settings are correct. Check the network Access Control List (ACL) and confirm that the adapter has adequate permissions to access the target.

3 Follow the prompts to complete the installation.

4 Reboot the host.

5 In the host BIOS settings, enter the iBFT adapter BIOS configuration, and change the adapter parameter to boot from the iSCSI target.

   See the vendor documentation for your system.

What to do next

On your iBFT adapter, reenable the option to boot to the iSCSI target, so the system will boot from the LUN you installled ESXi on.

Installing, Upgrading, or Migrating Hosts Using a Script

4

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

This chapter includes the following topics:

Approaches for Scripted Installation

You can install ESXi on multiple machines using a single script for all of them or a separate script for each machine.

For example, because disk names vary from machine to machine, one of the settings that you might want to configure in a script is the selection for the disk to install ESXi on.

Table 4-1. Scripted Installation Choices

Option	Action
Always install on the first disk on multiple machines.	Create one script.
Install ESXi on a different disk for each machine.	Create multiple scripts.

For information about the commands required to specify the disk to install on, see "Installation and Upgrade Script Commands," on page 53.

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 ESXi installer 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 61 and "PXE Booting the ESXi Installer," on page 20.

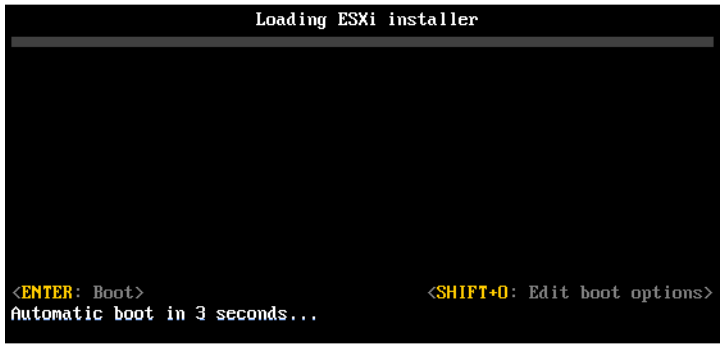
A `ks=...` option must be given, to specify the location of the installation script. Otherwise, a scripted installation or upgrade will not start. If `ks=...` is omitted, the text installer will proceed.

Supported boot options are listed in "Boot Options," on page 51.

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 4-2. 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`. An example using nfs protocol is `ks=nfs://`*host*`:`*porturl–path*. 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.

About the Default ks.cfg Installation Script

The ESXi installer includes a default installation script that performs a standard installation to the first detected disk.

The default `ks.cfg` installation script is located in the initial RAM disk at `/etc/vmware/weasel/ks.cfg`. You can specify the location of the default `ks.cfg` file with the `ks=file://etc/vmware/weasel/ks.cfg` boot option. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 50.

When you install ESXi using the `ks.cfg` script, the default root password is `mypassword`.

You cannot modify the default script on the installation media. After the installation, you can log in to the ESXi host and use the vSphere Client to modify the default settings.

The default script contains the following commands:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula

# Set the root password for the DCUI and Tech Support Mode
rootpw mypassword

# Install on the first local disk available on machine
install --firstdisk --overwritevmfs

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

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 19.
- USB Flash drive. See "Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script," on page 18.
- A network location accessible through 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 52.

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 50.

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 61.

`--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 61.

`--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 a version 4.x 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.

If you are upgrading a 5.0.x host, supported custom VIBs on the host that are not included in the ESXi installer ISO are migrated. If the host or the installer .ISO contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the offending VIB. You can remove the VIB and retry the upgrade, or use ESXI Image Builder to create a custom installer .ISO that resolves the conflict. The `forcemigrate` option is not available.

See the *vSphere Upgrade* documentation for imformation about upgrading hosts that have third-party custom VIBs.

.

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

serialnum or vmserialnum (optional)

Deprecated in ESXi 5.0.x. Supported in ESXi 5.1. Configures licensing. If not included, ESXi installs in evaluation mode.

--esx=<license-key>	Specifies the vSphere license key to use. The format is 5 five-character groups (*XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*).

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 61.

`--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 a version 4.x 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. If you are upgrading a 5.0.x host, supported custom VIBs that are not included in the ESXi installer ISO are migrated. You do not need to to use the `forcemigrate` option.

See the *vSphere Upgrade* documentation for imformation about upgrading hosts that have third-party custom VIBs.

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.x 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.x scripted installation and upgrade commands.

In ESXi 5.x, 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.x 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.x.
`bootloader`	Not supported in ESXi 5.x.
`esxlocation`	Deprecated and unused in ESXi.
`firewall`	Not supported in ESXi 5.x.
`firewallport`	Not supported in ESXi 5.x.

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.x.
serialnum	Deprecated in ESXi 5.0.x. Supported in ESXi 5.1.
vmserialnum	Deprecated in ESXi 5.0.x. Supported in ESXi 5.1.
timezone	Not supported in ESXi 5.x.
virtualdisk	Not supported in ESXi 5.x.
zerombr	Not supported in ESXi 5.x.
%firstboot	`--level` option not supported in ESXi 5.x.
%packages	Not supported in ESXi 5.x.

Disk Device Names

The `install`, `upgrade`, and `installorupgrade` installation script commands require the use of disk device names.

Table 4-3. 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.x, 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 4-4. 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 19, "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 23, "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 25, and "PXE Booting the ESXi Installer," on page 20.

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 19.

Prerequisites

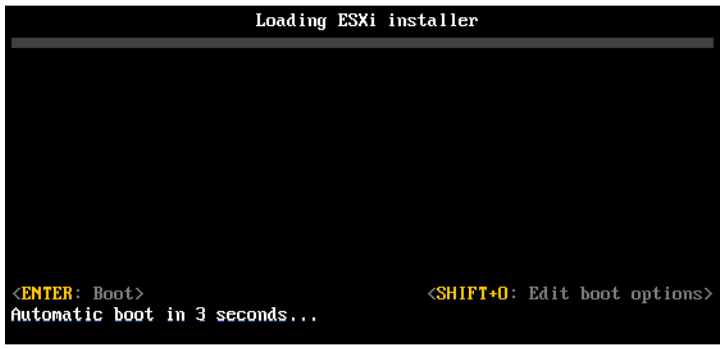
Before you run the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- The system on which you are installing, upgrading, or migrating meets the hardware requirements. See "ESXi Hardware Requirements," on page 29.
- 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 17.
- 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 52.
- 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 50. For a complete list of boot commands, see "Boot Options," on page 51.

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.

Supported boot options are listed in "Boot Options," on page 51.

Prerequisites

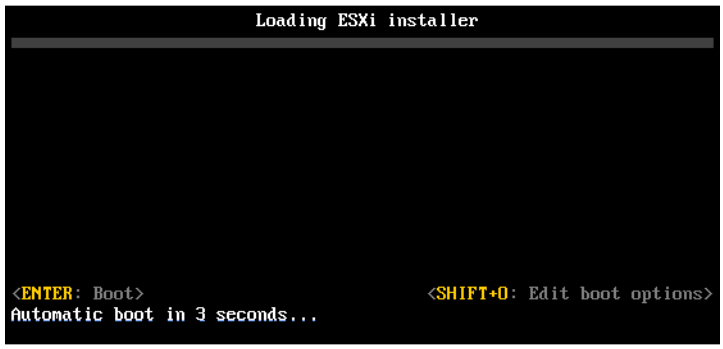
Before running the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- 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 29.
- 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 17.
- 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 52.
- 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 50.

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.x 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 20.
- For information about creating and locating an installation script, see "About Installation and Upgrade Scripts," on page 52.
- 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 25
  - "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 23
  - "PXE Boot the ESXi Installer Using gPXE," on page 26
- For information about using Auto Deploy to perform a scripted installation by PXE booting, see Chapter 5, "Installing ESXi Using vSphere Auto Deploy," on page 65.

Installing ESXi Using vSphere Auto Deploy

5

vSphere Auto Deploy lets you provision hundreds of physical hosts with ESXi software.

Using Auto Deploy, experienced system administrators can manage large deployments efficiently. Auto Deploy can be used for stateless caching or stateful installs.

Stateless caching By default, Auto Deploy does not store ESXi configuration or state on the host disk. Instead, an image profile defines the image that the host is provisioned with, and other host attributes are managed through host profiles.

Stateful installs You can provision a host with Auto Deploy and set up the host to store the image to disk. On subsequent boots, the host boots from disk.

This chapter includes the following topics:

Understanding vSphere Auto Deploy

vSphere Auto Deploy can provision hundreds of physical hosts with ESXi software. You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts, and a vCenter Server location (folder or cluster) for each host.

Introduction to Auto Deploy

When you start a physical host that is set up for Auto Deploy, Auto Deploy uses a PXE boot infrastructure in conjunction with vSphere host profiles to provision and customize that host. No state is stored on the host itself, instead, the Auto Deploy server manages state information for each host.

State Information for ESXi Hosts

Auto Deploy stores the information for the ESXi hosts to be provisioned in different locations. Information about the location of image profiles and host profiles is initially specified in the rules that map machines to image profiles and host profiles.

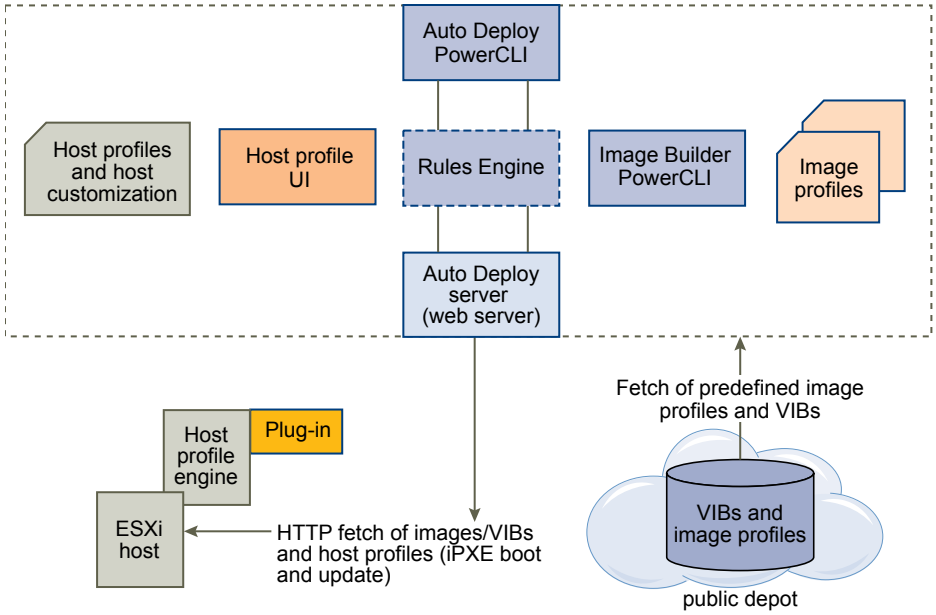
Table 5-1. Auto Deploy Stores Information for Deployment

Information Type	Description	Source of State Information
Image state	Executable software to run on an ESXi host.	Image profile, created with Image Builder PowerCLI.
Configuration state	Configurable settings that determine how the host is configured, for example, virtual switches and their settings, driver settings, boot parameters, and so on.	Host profile, created by using the host profile UI. Often comes from a template host.
Dynamic state	Runtime state that is generated by the running software, for example, generated private keys or runtime databases.	Stored in host memory and lost during reboot.
Virtual machine state	Virtual machines stored on a host and virtual machine autostart information (subsequent boots only).	vCenter Server must be available to supply virtual machine information to Auto Deploy.
User input	State that is based on user input, for example, an IP address that the user provides when the system starts up, cannot automatically be included in the host profile.	You can create a host profile that requires user input for certain values. When Auto Deploy applies a host profile that requires an answer to a host, the host comes up in maintenance mode. Use the host profiles interface to check the host profile compliance, and respond to the prompt to customize the host. The host customization information is stored with the host.

Auto Deploy Architecture

The Auto Deploy infrastructure consists of several components.

Figure 5-1. vSphere Auto Deploy Architecture



Auto Deploy server Serves images and host profiles to ESXi hosts. The Auto Deploy server is at the heart of the Auto Deploy infrastructure.

Auto Deploy rules engine Tells the Auto Deploy server which image profile and which host profile to serve to which host. Administrators use the Auto Deploy PowerCLI to define the rules that assign image profiles and host profiles to hosts.

Image profiles Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use the Image Builder PowerCLI to examine the depot and the Auto Deploy rules engine to specify which image profile to assign to which host.
- VMware customers can create a custom image profile based on the public image profiles and VIBs in the depot and apply that image profile to the host.

Host profiles Define machine-specific configuration such as networking or storage setup. Administrators create host profiles by using the host profile UI. You can create a host profile for a reference host and apply that host profile to other hosts in your environment for a consistent configuration.

Host customization Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. See "Host Customization in the vSphere Web Client," on page 113.

Host customization was called answer file in earlier releases of Auto Deploy.

Rules and Rule Sets

You specify the behavior of the Auto Deploy server by using a set of rules written in Power CLI. The Auto Deploy rules engine checks the rule set for matching host patterns to decide which items (image profile, host profile, or vCenter Server location) to provision each host with.

The rules engine maps software and configuration settings to hosts based on the attributes of the host. For example, you can deploy image profiles or host profiles to two clusters of hosts by writing two rules, each matching on the network address of one cluster.

For hosts that have not yet been added to a vCenter Server system, the Auto Deploy server checks with the rules engine before serving image profiles, host profiles, and inventory location information to hosts. For hosts that are managed by a vCenter Server system, the image profile, host profile, and inventory location that vCenter Server has stored in the host object is used. If you make changes to rules, you can use Auto Deploy PowerCLI cmdlets to test and repair rule compliance. When you repair rule compliance for a host, that host's image profile and host profile assignments are updated.

NOTE You must test and repair rule compliance for any host managed by a vCenter Server system even if those hosts were not added to the vCenter Server system by Auto Deploy. See "Test and Repair Rule Compliance," on page 85.

The rules engine includes rules and rule sets.

Rules Rules can assign image profiles and host profiles to a set of hosts, or specify the location (folder or cluster) of a host on the target vCenter Server system. A rule can identify target hosts by boot MAC address, SMBIOS information, BIOS UUID, Vendor, Model, or fixed DHCP IP address. In most cases, rules apply to multiple hosts. You create rules by using Auto Deploy PowerCLI cmdlets. After you create a rule, you must add it to a rule set. Only two rule sets, the active rule set and the working rule set, are supported. A rule can belong to both sets, the default, or only to the working rule set. After you add a rule to a rule set, you can no longer change the rule. Instead, you copy the rule and replace items or patterns in the copy. By default, Auto Deploy uses the name of the rule for the copy and hides the original rule.

Active Rule Set When a newly started host contacts the Auto Deploy server with a request for an image profile, the Auto Deploy server checks the active rule set for matching rules. The image profile, host profile, and vCenter Server inventory location that are mapped by matching rules are then used to boot the host. If more than one item of the same type is mapped by the rules, the Auto Deploy server uses the item that is first in the rule set.

Working Rule Set The working rule set allows you to test changes to rules before making the changes active. For example, you can use Auto Deploy PowerCLI cmdlets for testing compliance with the working rule set. The test verifies that hosts managed by a vCenter Server system are following the rules in the working rule set. By default, cmdlets add the rule to the working rule set and activate the rules. Use the `NoActivate` parameter to add a rule only to the working rule set.

You use the following workflow with rules and rule sets.

1. Make changes to the working rule set.
2. Use cmdlets that execute the working rule set rules against a host to make sure that everything is working correctly.
3. Refine and retest the rules in the working rule set.

4 Activate the rules in the working rule set.

   If you add a rule and do not specify the `NoActivate` parameter, all rules that are currently in the working rule set are activated. You cannot activate individual rules.

See the PowerCLI command-line help and "Managing Auto Deploy with PowerCLI Cmdlets," on page 82.

Auto Deploy Boot Process

When you boot a host that you want to provision or reprovision with vSphere Auto Deploy, the Auto Deploy infrastructure supplies the image profile and, optionally, a host profile and a vCenter Server location for that host.

The boot process is different for hosts that have not yet been provisioned with Auto Deploy (first boot) and for hosts that have been provisioned with Auto Deploy and added to a vCenter Server system (subsequent boot).

First Boot Prerequisites

Before a first boot process, you must set up your system. Setup includes the following tasks, which are discussed in more detail in "Preparing for vSphere Auto Deploy," on page 75.

- Set up a DHCP server that assigns an IP address to each host upon startup and that points the host to the TFTP server to download the iPXE boot loader from.
- Ensure that the Auto Deploy server has an IPv4 address. PXE booting is supported only with IPv4. Other components in your Auto Deploy infrastructure can communicate either with IPv4 or with IPv6.
- Identify an image profile to be used in one of the following ways.
  - Choose an ESXi image profile in a public depot.
  - (Optional) Create a custom image profile by using the Image Builder PowerCLI, and place the image profile in a depot that the Auto Deploy server can access. The image profile must include a base ESXi VIB.
- (Optional) If you have a reference host in your environment, export the host profile of the reference host and define a rule that applies the host profile to one or more hosts. See "Setting Up an Auto Deploy Reference Host," on page 97.
- Specify rules for the deployment of the host and add the rules to the active rule set.

First Boot Overview

When a host that has not yet been provisioned with vSphere Auto Deploy boots (first boot), the host interacts with several Auto Deploy components.

1 When the administrator turns on a host, the host starts a PXE boot sequence.

   The DHCP Server assigns an IP address to the host and instructs the host to contact the TFTP server.

2 The host contacts the TFTP server and downloads the iPXE file (executable boot loader) and an iPXE configuration file.

3 iPXE starts executing.

   The configuration file instructs the host to make a HTTP boot request to the Auto Deploy server. The HTTP request includes hardware and network information.

4 In response, the Auto Deploy server performs these tasks:

   a Queries the rules engine for information about the host.

   b Streams the components specified in the image profile, the optional host profile, and optional vCenter Server location information.

5 The host boots using the image profile.

If the Auto Deploy server provided a host profile, the host profile is applied to the host.

6 Auto Deploy adds the host to the vCenter Server system that Auto Deploy is registered with.

a If a rule specifies a target folder or cluster on the vCenter Server system, the host is placed in that folder or cluster. The target folder must be under a data center.

b If no rule exists that specifies a vCenter Server inventory location, Auto Deploy adds the host to the first datacenter displayed in the vSphere Client or in the vSphere Web Client UI.

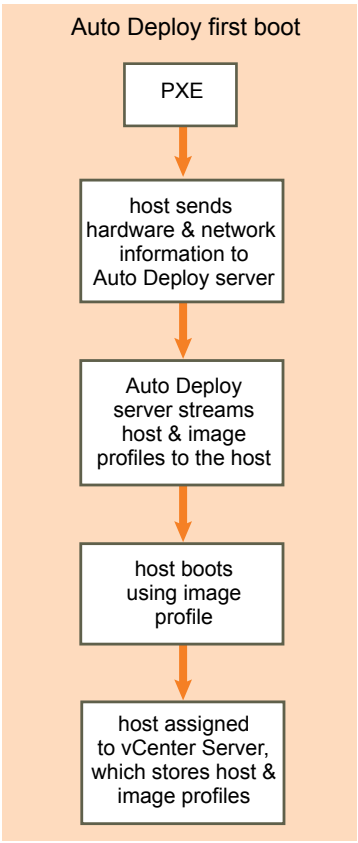
7 (Optional) If the host profile requires the user to specify certain information, such as a static IP address, the host is placed in maintenance mode when the host is added to the vCenter Server system.

You must reapply the host profile and answer any questions to have the host exit maintenance mode. See "Applying a Host Profile to Prompt for User Input in the vSphere Client," on page 89.

8 If the host is part of a DRS cluster, virtual machines from other hosts might be migrated to the host after the host has successfully been added to the vCenter Server system.

See "Provision a Host (First Boot)," on page 86.

Figure 5-2. Auto Deploy Installation, First Boot



Subsequent Boots Without Updates

For hosts that are provisioned with Auto Deploy and managed by a vCenter Server system, subsequent boots can become completely automatic.

1 The administrator reboots the host.

2 As the host boots up, Auto Deploy provisions the host with its image profile and host profile.

3 Virtual machines are brought up or migrated to the host based on the settings of the host.

- Standalone host. Virtual machines are powered on according to autostart rules defined on the host.
- DRS cluster host. Virtual machines that were successfully migrated to other hosts stay there. Virtual machines for which no host had enough resources are registered to the rebooted host.

If the vCenter Server system is unavailable, the host contacts the Auto Deploy and is provisioned with an image profile. The host continues to contact the Auto Deploy server until Auto Deploy reconnects to the vCenter Server system.

Auto Deploy cannot set up vSphere distributed switches if vCenter Server is unavailable, and virtual machines are assigned to hosts only if they participate in an HA cluster. Until the host is reconnected to vCenter Server and the host profile is applied, the switch cannot be created. Because the host is in maintenance mode, virtual machines cannot start. See "Reprovision Hosts with Simple Reboot Operations," on page 87.

Any hosts that are set up to require user input are placed in maintenance mode. See "Applying a Host Profile to Prompt for User Input in the vSphere Client," on page 89 and "Update the Host Customization in the vSphere Web Client," on page 89.

Subsequent Boots With Updates

You can change the image profile, host profile, or vCenter Server location for hosts. The process includes changing rules and testing and repairing the host's rule compliance.

1 The administrator uses the `Copy-DeployRule` PowerCLI cmdlet to copy and edit one or more rules and updates the rule set. See "Auto Deploy Roadmap," on page 72 for an example.

2 The administrator runs the `Test-DeployRulesetCompliance` cmdlet to check whether each host is using the information that the current rule set specifies.

3 The host returns a PowerCLI object that encapsulates compliance information.

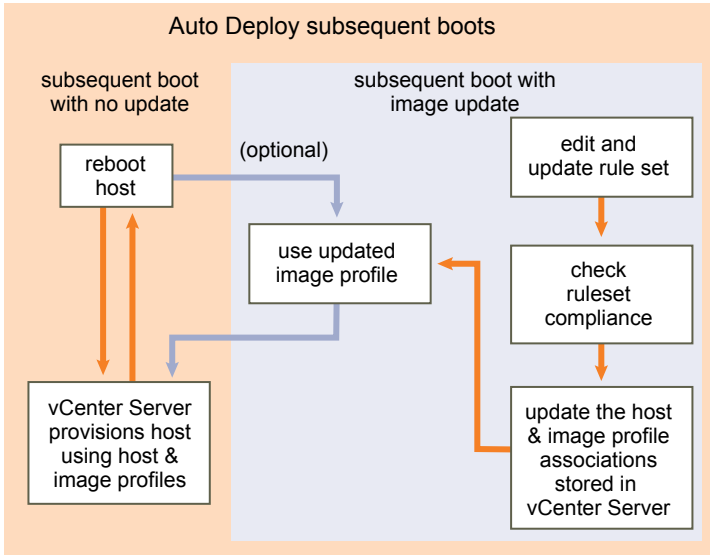
4 The administrator runs the `Repair-DeployRulesetCompliance` cmdlet to update the image profile, host profile, or vCenter Server location the vCenter Server system stores for each host.

5 When the host reboots, it uses the updated image profile, host profile, or vCenter Server location for the host.

   If the host profile is set up to request user input, the host is placed in maintenance mode. Follow the steps in "Applying a Host Profile to Prompt for User Input in the vSphere Client," on page 89 and "Update the Host Customization in the vSphere Web Client," on page 89.

See "Test and Repair Rule Compliance," on page 85.

Figure 5-3. Auto Deploy Installation, Subsequent Boots



Provisioning of Systems that Have Distributed Switches

You can configure the host profile of an Auto Deploy reference host with a distributed switch.

When you configure the distributed switch, the boot configuration parameters policy is automatically set to match the network parameters required for host connectivity after a reboot.

When Auto Deploy provisions the ESXi host with the host profile, the host goes through a two-step process.

1 The host creates a standard virtual switch with the properties specified in the boot configuration parameters field.

2 The host creates the VMkernel NICs. The VMkernel NICs allow the host to connect to Auto Deploy and to the vCenter Server system.

When the host is added to vCenter Server, vCenter Server removes the standard switch and reapplies the distributed switch to the host.

NOTE Do not change the boot configuration parameters to avoid problems with your distributed switch.

Auto Deploy Roadmap and Cmdlet Overview

To be successful with Auto Deploy, you have to know the tasks involved in provisioning hosts, understand the Auto Deploy components and their interaction, and know the PowerCLI cmdlets.

Auto Deploy Roadmap

Getting started with Auto Deploy requires that you learn how Auto Deploy works, install the Auto Deploy server, install PowerCLI, write PowerCLI rules that provision hosts, and turn on your hosts to be booted with the image profile you specify. Customizations of the image profile, host profile, and vCenter Server location are supported.

See "Auto Deploy Proof of Concept Setup," on page 128 for a step-by-step exercise that helps you set up your first Auto Deploy environment on a Windows 2008 system.

To successfully provision the hosts in your environment with Auto Deploy you can follow a few steps discussed in more detail in this document.

1 Install the Auto Deploy server.

Windows	The Auto Deploy server is included with the vCenter Server installation media. You can install the Auto Deploy server on the same system as vCenter Server or on a different system.
vCenter Server appliance	The vCenter Server appliance includes vCenter Server and the Auto Deploy server. The Auto Deploy server on the vCenter Server appliance is disabled by default. You can use both servers on the appliance, use a standalone vCenter Server installation with Auto Deploy on the appliance, or use a standalone Auto Deploy installation with the vCenter Server appliance. See "Using Auto Deploy with the VMware vCenter Server Appliance," on page 108 for configuration information.

NOTE You cannot use more than one Auto Deploy server with one vCenter Server system.

See "Prepare Your System and Install the Auto Deploy Server," on page 76 for information on installing the software, setting up the DHCP server, and downloading the TFTP configuration file.

2 Install PowerCLI, which includes Auto Deploy and Image Builder cmdlets, and set up remote signing.

See "Install PowerCLI and Prerequisite Software," on page 79 and "Using Auto Deploy Cmdlets," on page 79.

3 Find the image profile that includes the VIBs that you want to deploy to your hosts.

- In most cases, you add the depots that contain the software that you are interested in to your PowerCLI session, and then select an image profile from one of those depots.
- To create a custom image profile, use Image Builder cmdlets to clone an existing image profile and add the custom VIBs to the clone. Add the custom image profile to the PowerCLI session.

Using Image Builder for customization is required only if you have to add or remove VIBs. In most cases, you can add the depot where VMware hosts the image profiles to your PowerCLI session as a URL.

4 Use the `New-DeployRule` PowerCLI cmdlet to write a rule that assigns the image profile to one host, to multiple hosts specified by a pattern, or to all hosts.

```
New-DeployRule -Name "testrule" -Item image-profile -AllHosts
```

See "Assign an Image Profile to Hosts," on page 82.

NOTE Auto Deploy is optimized for provisioning hosts that have a fixed MAC address to IP address mapping in DHCP (sometimes called DHCP reservations). If you want to use static IP addresses, you must set up the host profile to prompt for host customization. See "Set Up Host Profiles for Static IP Addresses in the vSphere Client," on page 106 and "Set Up Host Profiles for Static IP Addresses in the vSphere Web Client," on page 107.

5 Turn on the host to have Auto Deploy provision the host with the specified image profile.

6 Set up the host you provisioned as a reference host for your host profile.

You can specify the reference host syslog settings, firewall settings, storage, networking, and so on. See "Setting Up an Auto Deploy Reference Host," on page 97.

7 Create and export a host profile for the reference host.

See the *Host Profiles* documentation.

8 To provision multiple hosts, you can use the `Copy-DeployRule` cmdlet.

You can revise the rule to assign not only an image profile but also a host profile and a cluster location .

```
Copy-DeployRule -DeployRule "testrule" -ReplaceItem
my_host_profile_from_reference_host,my_targetcluster
              -ReplacePattern  "ipv4=192.XXX.1.10-192.XXX.1.20"
```

my_host_profile_from_reference_host is the name of the reference host profile. *my_targetcluster* is the name of the target cluster.

9 Turn on the hosts you want to provision.

If the hosts that are specified by the pattern are not currently managed by a vCenter Server system, Auto Deploy provisions them with the already stored image profile and the specified host profile and adds them to the target cluster.

10 Check that the hosts you provisioned meet the following requirements.

- Each host is connected to the vCenter Server system.
- The hosts are not in maintenance mode.
- The hosts have no compliance failures.
- Each host with a host profile that requires user input has up-to-date host customization information.

Remedy host customization and compliance problems and reboot hosts until all hosts meet the requirements.

Read "Understanding vSphere Auto Deploy," on page 66 for an introduction to the boot process, a discussion of differences between first and subsequent boots, and an overview of using host customization.

Auto Deploy PowerCLI Cmdlet Overview

You specify the rules that assign image profiles and host profiles to hosts using a set of PowerCLI cmdlets that are included in VMware PowerCLI.

If you are new to PowerCLI, read the PowerCLI documentation and review "Using Auto Deploy Cmdlets," on page 79. You can get help for any command at the PowerShell prompt.

- Basic help: `Get-Help` *cmdlet_name*
- Detailed help: `Get-Help` *cmdlet_name* `-Detailed`

NOTE When you run Auto Deploy cmdlets, provide all parameters on the command line when you invoke the cmdlet. Supplying parameters in interactive mode is not recommended.

Table 5-2. Rule Engine PowerCLI Cmdlets

Command	Description
`Get-DeployCommand`	Returns a list of Auto Deploy cmdlets.
`New-DeployRule`	Creates a new rule with the specified items and patterns.
`Set-DeployRule`	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set.
`Get-DeployRule`	Retrieves the rules with the specified names.
`Copy-DeployRule`	Clones and updates an existing rule.
`Add-DeployRule`	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the `NoActivate` parameter to add a rule only to the working rule set.

Table 5-2. Rule Engine PowerCLI Cmdlets (Continued)

Command	Description
`Remove-DeployRule`	Removes one or more rules from the working rule set and from the active rule set. Run this command with the `-Delete` parameter to completely delete the rule.
`Set-DeployRuleset`	Explicitly sets the list of rules in the working rule set.
`Get-DeployRuleset`	Retrieves the current working rule set or the current active rule set.
`Switch-ActiveDeployRuleset`	Activates a rule set so that any new requests are evaluated through the rule set.
`Get-VMHostMatchingRules`	Retrieves rules matching a pattern. For example, you can retrieve all rules that apply to a host or hosts. Use this cmdlet primarily for debugging.
`Test-DeployRulesetCompliance`	Checks whether the items associated with a specified host are in compliance with the active rule set.
`Repair-DeployRulesetCompliance`	Given the output of `Test-DeployRulesetCompliance`, this cmdlet updates the image profile, host profile, and location for each host in the vCenter Server inventory. The cmdlet might apply image profiles, apply host profiles, or move hosts to prespecified folders or clusters on the vCenter Server system.
`Apply-EsxImageProfile`	Associates the specified image profile with the specified host.
`Get-VMHostImageProfile`	Retrieves the image profile in use by a specified host. This cmdlet differs from the `Get-EsxImageProfile` cmdlet in the Image Builder PowerCLI.
`Repair-DeployImageCache`	Use this cmdlet only if the Auto Deploy image cache is accidentally deleted.
`Get-VMHostAttributes`	Retrieves the attributes for a host that are used when the Auto Deploy server evaluates the rules.
`Get-DeployMachineIdentity`	Returns a string value that Auto Deploy uses to logically link an ESXi host in vCenter to a physical machine.
`Set-DeployMachineIdentity`	Logically links a host object in the vCenter Server database to a physical machine. Use this cmdlet to add hosts without specifying rules.
`Get-DeployOption`	Retrieves the Auto Deploy global configuration options. This cmdlet currently supports the `vlan-id` option, which specifies the default VLAN ID for the ESXi Management Network of a host provisioned with Auto Deploy. Auto Deploy uses the value only if the host boots without a host profile.
`Set-DeployOption`	Sets the value of a global configuration option. Currently supports the `vlan-id` option for setting the default VLAN ID for the ESXi Management Network.

Preparing for vSphere Auto Deploy

Before you can start to use vSphere Auto Deploy, you must prepare your environment. You start with server setup and hardware preparation. You must register the Auto Deploy software with the vCenter Server system that you plan to use for managing the hosts you provision, and install the VMware PowerCLI.

- Prepare Your System and Install the Auto Deploy Server on page 76

  Before you turn on a host for PXE boot with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that Auto Deploy interacts with.

- Install PowerCLI and Prerequisite Software on page 79

  Before you can run Auto Deploy cmdlets to create and modify the rules and rule sets that govern Auto Deploy behavior, you must install vSphere PowerCLI and all prerequisite software. The Auto Deploy cmdlets are included with the PowerCLI installation.

- Using Auto Deploy Cmdlets on page 79

  Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in vSphere PowerCLI. Users of Auto Deploy cmdlets can take advantage of all PowerCLI features.

- Set Up Bulk Licensing on page 80

  You can use the vSphere Client, the vSphere Web Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with Auto Deploy.

Prepare Your System and Install the Auto Deploy Server

Before you turn on a host for PXE boot with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that Auto Deploy interacts with.

Prerequisites

- Ensure that the hosts that you will provision with Auto Deploy meet the hardware requirements for ESXi 5.1.

  See "ESXi Hardware Requirements," on page 29.

  NOTE You cannot provision EFI hosts with Auto Deploy unless you switch the EFI system to BIOS compatibility mode.

- Ensure that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met.

  See "Required Ports for vCenter Server," on page 39.

- If you want to use VLANs in your Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the UNDI driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the BIOS. You must also correctly configure the ESXi port groups with the correct VLAN IDs. Ask your network administrator how VLAN IDs are used in your environment.

- Ensure that you have enough storage for the Auto Deploy repository. The Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.

  Best practice is to allocate 2GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350MB. Determine how much space to reserve for the Auto Deploy repository by considering how many image profiles you expect to use.

- Obtain the vCenter Server installation media, which include the Auto Deploy installer, or deploy the vCenter Server Appliance.

  See Chapter 11, "Installing vCenter Server," on page 245.

  See "Using Auto Deploy with the VMware vCenter Server Appliance," on page 108.

- Ensure that a TFTP server is available in your environment. If you require a supported solution, purchase a supported TFTP server from your vendor of choice.

- Obtain administrative privileges to the DHCP server that manages the network segment you want to boot from. You can use a DHCP server already in your environment, or install a DHCP server. For your Auto Deploy setup, replace the `gpxelinux.0` file name with `undionly.kpxe.vmw-hardwired`.

- Secure your network as you would for any other PXE-based deployment method. Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or the Auto Deploy server is not checked during a PXE boot. .

  NOTE Auto Deploy is not supported with NPIV (N_Port ID Virtualization).

- Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.
- Install ESXi Dump Collector and set up your first host so all core dumps are directed to ESXi Dump Collector and apply the host profile from that host to all other hosts. See "Configure ESXi Dump Collector with ESXCLI," on page 99 and "Set Up ESXi Dump Collector from the Host Profiles Interface in the vSphere Client," on page 100.

  See "Install or Upgrade vSphere ESXi Dump Collector," on page 287.
- Auto Deploy does not support a pure IPv6 environment because the PXE boot specifications do not support IPv6. However, after the initial PXE boot state, the rest of the communication can happen over IPv6. You can register Auto Deploy to the vCenter Server system with IPv6, and you can set up the host profiles to bring up hosts with IPv6 addresses. Only the initial boot process requires an IPv4 address.

Procedure

1 Install the vSphere Auto Deploy server as part of a vCenter Server installation or standalone on a Windows system, or deploy the vCenter Server Appliance to an ESXi system of your choice.

Location	Description
vCenter Server system	Use the vCenter Server installation media to install Auto Deploy on the same host as the vCenter Server system itself. That vCenter Server system manages all hosts that you provision with this Auto Deploy installation. See "Install or Upgrade vSphere Auto Deploy," on page 289.
Windows system	Use the vCenter Server installation media to install Auto Deploy on a Microsoft Windows system that does not have a vCenter Server system installed. The installer prompts you for a vCenter Server system to register Auto Deploy with. That vCenter Server system manages all hosts that you provision with this Auto Deploy installation. See "Install or Upgrade vSphere Auto Deploy," on page 289.
vCenter Server Appliance	Deploy the vCenter Server Appliance to the ESXi host of your choice. The appliance includes an Auto Deploy server, which is disabled by default. By default, the vCenter Server system on the appliance manages all hosts you provision with the appliance Auto Deploy installation. Other configurations are supported. See "Using Auto Deploy with the VMware vCenter Server Appliance," on page 108.

2 Configure the TFTP server.

Option	Description
vSphere Client	a In a vSphere Client connected to the vCenter Server system that Auto Deploy is registered with, click **Home** in the navigation bar and select **Auto Deploy** in the Administration tab to display the Auto Deploy page. b Click **Download TFTP ZIP** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.
vSphere Web Client	a In a vSphere Web Client connected to the vCenter Server system that Auto Deploy is registered with, go to the inventory list and select the vCenter Server system. b Click the Manage tab, select Settings, and click Auto Deploy. c Click **Download TFTP Boot Log** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.

3 Set up your DHCP server to point to the TFTP server on which the TFTP ZIP file is located.

   a Specify the TFTP Server's IP address in DHCP option 66 (frequently called `next-server`).

   b Specify the boot file name, which is `undionly.kpxe.vmw-hardwired` in the DHCP option 67 (frequently called `boot-filename`).

4 Set each host you want to provision with Auto Deploy to network boot or PXE boot, following the manufacturer's instructions.

5 Locate the image profile that you want to use and the depot in which it is located.

   In most cases, you point to an image profile that VMware makes available in a public depot. If you want to include custom VIBs with the base image, you can use the Image Builder PowerCLI to create an image profile and use that image profile. See the *Image Builder PowerCLI* documentation.

6 Write a rule that assigns an image profile to hosts.

7 (Optional) You can use your own Certificate Authority (CA) by replacing the OpenSSL certificate (`rbd-ca.crt`) and the OpenSSL private key (`rbd-ca.key`) with your own certificate and key file.

   - On Windows, the files are in the SSL subfolder of the Auto Deploy installation directory. For example, on Windows 7 the default is `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.
   - On the vCenter Server Appliance, the files are in `/etc/vmware-rbd/ssl/`.

When you start a host that is set up for Auto Deploy, the host contacts the DHCP server and is directed to the Auto Deploy server, which provisions the host with the image profile specified in the active rule set.

What to do next

- Install PowerCLI. See "Install PowerCLI and Prerequisite Software," on page 79.
- Use the PowerCLI cmdlets to define a rule that assigns an image profile and optional host profile to the host. See "Prepare Your System and Install the Auto Deploy Server," on page 76.
- (Optional) Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- If you want to have Auto Deploy overwrite existing partitions, set up a reference host to do auto partitioning and apply the host profile of the reference host to other hosts. See "Consider and Implement Your Partitioning Stategy," on page 105.
- If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. See "Customizing Hosts with Answer Files in the vSphere Client," on page 110.

Install PowerCLI and Prerequisite Software

Before you can run Auto Deploy cmdlets to create and modify the rules and rule sets that govern Auto Deploy behavior, you must install vSphere PowerCLI and all prerequisite software. The Auto Deploy cmdlets are included with the PowerCLI installation.

You install vSphere PowerCLI and prerequisite software on a Microsoft Windows system. See the Microsoft Web site for information about installing the Microsoft software. See the *vSphere PowerCLI Installation Guide* for detailed instructions for PowerCLI installation.

Procedure

1 Verify that Microsoft .NET 2.0 is installed, or install it from the Microsoft Web site following the instructions on that Web site.

2 Verify that Microsoft Powershell 2.0 is installed, or install it from the Microsoft Web site following the instructions on that Web site.

3 Install vSphere vSphere PowerCLI, which includes the Auto Deploy cmdlets.

What to do next

Review "Using Auto Deploy Cmdlets," on page 79. If you are new to PowerCLI, read the PowerCLI documentation.

Use Auto Deploy cmdlets and other PowerCLI cmdlets and PowerShell cmdlets to manage Auto Deploy rules and rule sets. Use `Get-Help <cmdlet_name>` at any time for command-line help.

Using Auto Deploy Cmdlets

Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in vSphere PowerCLI. Users of Auto Deploy cmdlets can take advantage of all PowerCLI features.

Experienced PowerShell users can use Auto Deploy cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and PowerCLI, the following tips might be helpful.

You can type cmdlets, parameters, and parameter values in the PowerCLI shell.

- Get help for any cmdlet by running **`Get-Help`** ***`cmdlet_name`***.
- Remember that PowerShell is not case sensitive.
- Use tab completion for cmdlet names and parameter names.
- Format any variable and cmdlet output by using **`Format-List`** or **`Format-Table`** or their short forms **`fl`** or **`ft`**. See **`Get-Help Format-List`**.

Passing Parameters by Name

You can pass in parameters by name in most cases and surround parameter values that contain spaces or special characters with double quotes.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Most examples in the documentation pass in parameters by name.

Passing Parameters as Objects

You can pass parameters as objects if you want to do scripting and automation. Passing in parameters as objects is useful with cmdlets that return multiple objects and with cmdlets that return a single object. Consider the following example.

1 Bind the object that encapsulates rule set compliance information for a host to a variable.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

2 Display the `itemlist` property of the object to see the difference between what is in the rule set and what the host is currently using.

```
$tr.itemlist
```

3 Remediate the host to use the revised rule set by passing the object to a call to `Repair-DeployRuleSetCompliance`.

```
Repair-DeployRuleSetCompliance $tr
```

The example remediates the host the next time you boot the host.

Setting Properties to Support Remote Signing

For security reasons, Windows PowerShell supports an execution policy feature. It determines whether scripts are allowed to run and whether they must be digitally signed. By default, the execution policy is set to Restricted, which is the most secure policy. If you want to run scripts or load configuration files, you can change the execution policy by using the `Set-ExecutionPolicy` cmdlet. To do this, type the following in the vSphere PowerCLI console window.

```
Set-ExecutionPolicy RemoteSigned
```

If the command is successful, you can run scripts and load configuration files. For more information about the execution policy and digital signing in Windows PowerShell, use the following command.

```
Get-Help About_Signing
```

Set Up Bulk Licensing

You can use the vSphere Client, the vSphere Web Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with Auto Deploy.

The following example assigns licenses to all hosts in a data center. You can also associate licenses with hosts and clusters.

The following example is for advanced PowerCLI users who know how to use PowerShell variables.

Prerequisites

Install PowerCLI. See "Install PowerCLI and Prerequisite Software," on page 79.

Assigning license keys through the vSphere Client or vSphere Web Client and assigning licensing by using PowerCLI cmdlets function differently.

Assign license keys with vSphere Client or the vSphere Web Client	You can assign license keys to a host when you add the host to the vCenter Server system or when the host is managed by a vCenter Server system.
Assign license keys with LicenseDataManager PowerCLI	You can specify a set of license keys to be added to a set of hosts. The license keys are added to the vCenter Server database. Each time a host is added to the vCenter Server system or reconnects to the vCenter Server system, the host is assigned a license key. A license key that is assigned through the PowerCLI is treated as a default license key. When an unlicensed host is added or reconnected, it is assigned the default license key. If a host is already licensed, it keeps its license key.

Procedure

1 Connect to the vCenter Server system you want to use and bind the associated license manager to a variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2 Run a cmdlet that retrieves the datacenter in which the hosts for which you want to use the bulk licensing feature are located.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

You can also run a cmdlet that retrieves a cluster to use bulk licensing for all hosts in a cluster, or retrieves a folder to use bulk licensing for all hosts in a folder.

3 Create a new `LicenseData` object and a `LicenseKeyEntry` object with associated type ID and license key.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere"
$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

4 Associate the `LicenseKeys` attribute of the `LicenseData` object you created in step 3 with the `LicenseKeyEntry` object.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

5 Update the license data for the data center with the `LicenseData` object and verify that the license is associated with the host container.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
$licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

6 Provision one or more hosts with Auto Deploy and assign them to the data center or to the cluster that you assigned the license data to.

7 You can use the vSphere Client or the vSphere Web Client to verify that the host is successfully assigned to the default license `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`.

All hosts that you assigned to the data center are now licensed automatically.

Managing Auto Deploy with PowerCLI Cmdlets

You can use Auto Deploy PowerCLI cmdlets to create rules that associate hosts with image profiles, host profiles, and a location on the vCenter Server target. You can also update hosts by testing rule compliance and repairing compliance issues.

Assign an Image Profile to Hosts

Before you can provision a host, you must create rules that assign an image profile to each host that you want to provision by using Auto Deploy.

Prerequisites

- Install VMware PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Auto Deploy Cmdlets," on page 79.

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 Determine the location of a public software depot, or define a custom image profile using 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. b Run **Add-EsxSoftwareDepot C:*file_path**my_offline_depot*.zip**.

4 In the depot, find the image profile that you want to use by running the `Get-EsxImageProfile` cmdlet.

By default, the ESXi depot includes one base image profile that includes VMware tools and has the string `standard` in its name, and one base image profile that does not include VMware tools.

5 Define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the image profile.

```
New-DeployRule -Name "testrule" -Item "My Profile25" -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Double quotes are required if a name contains spaces, optional otherwise. Specify `-AllHosts` instead of a pattern to apply the item to all hosts.

The cmdlet creates a rule named `testrule`. The rule assigns the image profile named My Profile25 to all hosts with a vendor of Acme or Zven that also have an IP address in the specified range.

6 Add the rule to the rule set.

```
Add-DeployRule testrule
```

By default, the rule is added to both the working rule set and the active rule set. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

When the host boots from iPXE, it reports attributes of the machine to the console. Use the same format of the attributes when writing deploy rules.

```
**********************************************************************
* Booting through VMware AutoDeploy...
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:Xa:Xb:Xc:Xx:XX
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . vendor=MyVendor
**********************************************************************
```

What to do next

- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new image profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new image profile.

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 85.

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 "Using Auto Deploy Cmdlets," on page 79.

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 Using the vSphere Client or the vSphere Web Client, set up a host with the settings you want to use and create a host profile from that host.

3 Find the name of the host profile by running `Get-VMhostProfile` PowerCLI cmdlet, passing in the ESXi host from which you create a host profile.

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 85.
- Turn on unprovisioned hosts to provision them with the host profile.

Assign a Host to a Folder or Cluster

Auto Deploy can assign a host to a folder or cluster. When the host boots, Auto Deploy adds it to the specified location on the vCenter Server. Hosts assigned to a cluster inherit the cluster's host profile.

The following procedure explains how to write a rule that assigns a host to a folder or cluster. To assign a host already provisioned with Auto Deploy to a new folder or cluster, you must also perform a test and repair cycle. See "Test and Repair Rule Compliance," on page 85.

NOTE The folder you select must be in a datacenter or in a cluster. You cannot assign the host to a standalone top-level folder.

Prerequisites

- Install VMware PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Auto Deploy Cmdlets," on page 79.

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 Define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to a folder or a cluster.

```
New-DeployRule -Name "testrule3" -Item "my folder" -Pattern "vendor=Acme,Zven", "ipv4=192.XXX.
1.10-192.XXX.1.20"
```

This example passes in the folder by name. You can instead pass in a folder, cluster, or datacenter object that you retrieve with the `Get-Folder`, `Get-Cluster`, or `Get-Datacenter` cmdlet.

3 Add the rule to the rule set.

```
Add-DeployRule testrule3
```

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 be added to the specified vCenter Server location by performing test and repair compliance operations on those hosts. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to add them to the specified vCenter Server location.

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 vSphere PowerCLI can access those ESXi hosts.

Prerequisites

- Install vSphere PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Auto Deploy Cmdlets," on page 79.

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. By default, PowerCLI uses the old name for the copy and hides the old rule.

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.

Provisioning ESXi Systems with vSphere Auto Deploy

vSphere Auto Deploy can provision hundreds of physical hosts with ESXi software. You can provision hosts that did not previously run ESXi software (first boot), reboot hosts, or reprovision hosts with a different image profile, host profile, or folder or cluster location.

The Auto Deploy process differs depending on the state of the host and on the changes that you want to make.

Provision a Host (First Boot)

Provisioning a host that has never been provisioned with Auto Deploy (first boot) differs from subsequent boot processes. You must prepare the host and fulfill all other prerequisites before you can provision the host. You can optionally define a custom image profile with Image Builder PowerCLI cmdlets.

Prerequisites

- Make sure your host meets the hardware requirements for ESXi hosts.

  See "ESXi Hardware Requirements," on page 29.

- Prepare the system for vSphere Auto Deploy (see "Preparing for vSphere Auto Deploy," on page 75).
- Write rules that assign an image profile to the host and optionally assign a host profile and a vCenter Server location to the host. See "Managing Auto Deploy with PowerCLI Cmdlets," on page 82.

  When setup is complete, the Auto Deploy server and PowerCLI are installed, DHCP setup is complete, and rules for the host that you want to provision are in the active rule set.

Procedure

1 Turn on the host.

  The host contacts the DHCP server and downloads iPXE from the location the server points it to. Next, the Auto Deploy server provisions the host with the image specified by the rule engine. The Auto Deploy server might also apply a host profile to the host if one is specified in the rule set. Finally, Auto Deploy adds the host to the vCenter Server system that is specified in the rule set.

2 (Optional) If Auto Deploy applies a host profile that requires user input such as an IP address, the host is placed in maintenance mode. Reapply the host profile with the vSphere Client or the vSphere Web Client and provide the user input when prompted.

After the first boot process, the host is running and managed by a vCenter Server system. The vCenter Server stores the host's image profile, host profile, and location information.

You can now reboot the host as needed. Each time you reboot, the host is reprovisioned by the vCenter Server system.

What to do next

Reprovision hosts as needed. See "Reprovisioning Hosts," on page 87.

If you want to change the image profile, host profile, or location of the host, update the rules and perform a test and repair compliance operation. See "Test and Repair Rule Compliance," on page 85.

Reprovisioning Hosts

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image profile 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 "Preparing for vSphere Auto Deploy," on page 75.

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 profile 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 Reboot the host.

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 compliance 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.
- During testing, you can 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 to boot the host with. Use the Image Builder PowerCLI, discussed in Chapter 6, "Using vSphere ESXi Image Builder CLI," on page 145.
- 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 `Get-EsxImageProfile` to see a list of image profiles, and decide which profile you want to use.

5 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
```

6 Test and repair rule compliance for each host that you want to deploy the image to.

See "Test and Repair Rule Compliance," on page 85.

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 in the vSphere Client

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 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

3 Select the host profile that requires user input when prompted.

4 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.

Update the Host Customization in the vSphere Web Client

If a host required user input during a previous boot, the answers are saved with the vCenter Server. If you want to prompt the user for new information, you remediate the host.

Prerequisites

Attach a host profile that prompts for user input to the host.

Procedure

1 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 Web Client, remediate the host.

a Right click the host and click **All vCenter Actions > Host Profiles > Remediate**.

3 When prompted, provide the user input.

You can now direct the host to exit maintenance mode.

The host customization is saved. The next time you boot, the host customization is applied to the host.

Using Auto Deploy for Stateless Caching and Stateful Installs

The Auto Deploy stateless caching feature allows you to cache the host's image locally on the host or on a network drive and continue to provision the host with Auto Deploy. The Auto Deploy stateful installs feature allows you to install hosts over the network without setting up a complete PXE boot infrastructure. After the initial network boot, these hosts boot like other hosts on which ESXi has been installed.

Introduction

The System Cache Configuration host profile supports stateless caching and stateful installs.

Stateless caching is a good solution when you use the Auto Deploy infrastructure, but you require a safeguard in case the Auto Deploy server is unavailable. Hosts provisioned with stateless caching host profile settings continue to be provisioned with Auto Deploy. Stateful installs support network installation through Auto Deploy. After the initial installation, hosts that are provisioned with stateful install host profile settings will boot from disk.

Use Cases

The System Cache Configuration host profile supports the following use cases.

Hosts provisioned with Auto Deploy cache the image (stateless caching)	Set up and apply a host profile for stateless caching. You can cache the image on a local disk, a remote disk, or a USB drive. Continue provisioning this host with Auto Deploy. If the Auto Deploy server becomes unavailable, the host boots from the cache.
Hosts provisioned with Auto Deploy become stateful hosts	Set up and apply a host profile for stateful installs. When you provision a host with Auto Deploy, the image is installed on the local disk, a remote disk, or a USB drive. For subsequent boots, you boot from disk. The host no longer uses Auto Deploy.

Preparation

To successfully use stateless caching or stateful installs, decide how to set up the system and set the boot order.

Table 5-3. Preparation for Stateless Caching or Stateful Installs

Requirement or Decision	Description
Decide on VMFS partition overwrite	When you install ESXi with the interactive installer, you are prompted whether you want to overwrite an existing VMFS datastore. The System Cache Configuration host profile allows you to overwrite existing VMFS partitions by selecting a check box. The check box is not available if you set up the host profile to use a USB drive.
Decide whether you need a highly available environment	If you use Auto Deploy with stateless caching, you can set up a highly available Auto Deploy environment to guarantee that virtual machines are migrated on newly provisioned hosts and that the environment supports vNetwork Distributed Switch even if the vCenter Server becomes temporarily available.
Set the boot order	The boot order you specify for your hosts depends on the feature you want to use. ■ To set up Auto Deploy with stateless caching, configure your host to first attempt to boot from the network, and to then attempt to boot from disk. If Auto Deploy is not available, the host boots using the cache. ■ To set up Auto Deploy for stateful installs on hosts that do not currently have a bootable disk, configure your hosts to first attempt to boot from disk, and to then attempt to boot from the network. NOTE If you currently have a bootable image on the disk, configure the hosts for one-time PXE boot and provision the host with Auto Deploy to use a host profile that specifies stateful installs.

Stateless Caching and Loss of Connectivity

If the ESXi hosts that run your virtual machines lose connectivity to the Auto Deploy server, the vCenter Server system, or both, some limitations apply when you next reboot.

- If vCenter Server is available but the Auto Deploy server is unavailable, hosts do not connect to the vCenter Server automatically. You can manually connect the hosts to the vCenter Server, or wait until the Auto Deploy server is available again.
- If both vCenter Server and vSphere Auto Deploy do not work, You can connect to each ESXi host by using the vSphere Client, and assign virtual machines to each host.
- If vCenter Server is not available, vSphere DRS does not work. The Auto Deploy server cannot add hosts to the vCenter Server system. You can connect to each ESXi host by using the vSphere Client, and assign virtual machines to each host.
- If you make changes to your setup while connectivity is lost, you lose these changes when the Auto Deploy server is restored after the outage.

Understanding Stateless Caching and Stateful Installs

When you want to use Auto Deploy with stateless caching or stateful installs, you must set up a host profile, apply the host profile, and set the boot order.

When you apply a host profile that enables caching to a host, Auto Deploy partitions the specified disk. What happens next depends on how you set up the host profile and how you set the boot order on the host.

- With the **Enable stateless caching on the host** host profile, Auto Deploy caches the image when you apply the host profile. No reboot is required. When you later reboot, the host continues to use the Auto Deploy infrastructure to retrieve its image. If the Auto Deploy server is not available, the host uses the cached image.
- With the **Enable stateful installs on the host** host profile, Auto Deploy installs the image. When you reboot the host, the host boots from disk, just like a host that was provisioned with the installer. Auto Deploy no longer provisions the host.

You can apply the host profile from a vSphere Client or from a vSphere Web Client, or write an Auto Deploy PowerCLI rule that applies the host profile.

Each workflow supports stateless caching and stateful installs.

Table 5-4. Workflows that set up hosts for stateless caching or stateful installs

Workflow	Stateless caching	Stateful install
Apply host profile from vSphere Client or vSphere Web Client	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. No reboot required.	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. Reboot is required.
Write and apply PowerCLI rule	Set up a reference host with a host profile that has the caching setup you want. Write a PowerCLI rule that provisions the host by using Auto Deploy and that applies a host profile that is set up for stateless caching. Reboot is required.	Set up a reference host with a host profile that has the caching setup you want. Write a PowerCLI rule that provisions the host by using Auto Deploy and applies a host profile that is set up for stateful installs. Reboot is required.

Applying the System Cache Configuration Host Profile from the vSphere Client or the vSphere Web Client

You can create a host profile on a reference host and apply that host profile to additional hosts or to a vCenter Server folder or cluster. The following workflow results.

1 You provision a host with Auto Deploy and edit that host's System Image Cache Configuration host profile.

2 You place one or more target hosts in maintenance mode, apply the host profile to each host, and instruct the host to exit maintenance mode.

3 What happens next depends on the host profile you selected.

   - If the host profile enabled stateless caching, the image is cached to disk. No reboot is required.
   - If the host profile enabled stateful installs, the image is installed. When you reboot, the host uses the installed image.

4 A reboot is required so the changes can take effect.

Applying the System Cache Configuration with PowerCLI

You can create a host profile for a reference host and write an Auto Deploy PowerCLI rule that applies that host profile to other target hosts. The following workflow results.

1 You provision a reference with Auto Deploy and create a host profile to enable a form of caching.

2 You write a rule that provisions additional hosts with Auto Deploy and that applies the host profile of the reference host to those hosts.

3 Auto Deploy provisions each host with the new image profile. The exact effect of applying the host profile depends on the host profile you selected and on whether the host was previously provisioned with Auto Deploy.

Table 5-5. First Boot and Subsequent Boots Comparison

First Boot	Subsequent Boots
For stateful installs, Auto Deploy installs the image.	For stateful installs, the host boots from disk.
For stateless caching, Auto Deploy provisions the host and caches the image.	For stateless caching, Auto Deploy provisions the host. ■ If Auto Deploy provisioned the host before but stateless caching was not set up before, Auto Deploy caches the image. ■ If Auto Deploy provided the host before and cached the image, Auto Deploy provisions the host using the information in the rules. ■ If Auto Deploy is unavailable, the host boots from the cached image.

Set Up Stateless Hosts to Use Auto Deploy with Caching

You can set up your system to provision hosts with Auto Deploy, and configure the hosts to use stateless caching. If the Auto Deploy server is not available when a host reboots, the host uses the cached image.

A host that is set up for stateless caching uses the cached image only if the Auto Deploy server is not available when the host reboots. In all other situations, the host is provisioned with Auto Deploy. If you change the rule that applies an image profile to the host, and you perform a test and repair compliance operation, Auto Deploy provisions the host with the new image and the new image is cached.

Set up a highly available Auto Deploy infrastructure to guarantee that virtual machines are migrated to the host if the host reboots. Because vCenter Server assigns virtual machines to the host, vCenter Server must be available. See "Set up a Highly Available Auto Deploy Infrastructure," on page 120.

You can set up your environment for stateless caching by applying host profiles directly or by using PowerCLI rules.

Table 5-6. Setting up hosts for stateless caching or stateful installs

Workflow	Stateless caching	Stateful install
Apply host profile directly	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. See "Configure a Host Profile to Use Stateless Caching," on page 94.	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. See "Configure a Host Profile to Enable Stateful Installs," on page 96.
Write and apply PowerCLI rules	Set up a reference host with a host profile that has the caching setup you want. Write an Auto Deploy PowerCLI rule that provisions the host and that applies a host profile that is set up for stateless caching. See "Assign a Host Profile to Hosts," on page 83.	Set up a reference host with a host profile that has the caching setup you want. Write an Auto Deploy PowerCLI rule that provisions the host and that applies a host profile that is set up for stateful installs. See "Assign a Host Profile to Hosts," on page 83.

Prepare for Auto Deploy with Stateless Caching

Before you can start provisioning a host that uses stateless caching with Auto Deploy, you must verify that your environment is set up for Auto Deploy, prepare Auto Deploy PowerCLI rules, and set the host boot order.

Prerequisites

- Decide which disk to use for caching and determine whether the caching process will overwrite an existing VMFS partition.
- In production environments, protect the vCenter Server system and the Auto Deploy server by including them in a highly available environment. Having the vCenter Server in a management cluster guarantees that VDS and virtual machine migration are available. If possible, protect other elements of your infrastructure. See "Set up a Highly Available Auto Deploy Infrastructure," on page 120.

Procedure

1 Set up your environment for Auto Deploy and install PowerCLI.

  See "Preparing for vSphere Auto Deploy," on page 75.

2 Verify that a disk with at least 1GB of free space is available.

  If the disk is not yet partitioned, partitioning happens when you apply the host profile.

3 Set up the host to first attempt a network boot and to boot from disk if network boot fails.

  See your hardware vendor's documentation.

What to do next

Set up a host profile for stateless caching. In most cases, you set up the host profile on a reference host and apply that host profile to other hosts.

Configure a Host Profile to Use Stateless Caching

When a host is set up to use stateless caching, the host uses a cached image if the Auto Deploy Server is not available. To use stateless caching, you must configure a host profile. You can apply that host profile to other hosts that you want to set up for stateless caching.

You can configure the host profile on a single host that you want to set up to use caching. You can also create a host profile that uses caching on a reference host and apply that host profile to other hosts.

Prerequisites

Prepare your host for stateless caching. See "Prepare for Auto Deploy with Stateless Caching," on page 94.

Procedure

1 In the vSphere Web Client, create a host profile.

  See the *Host Profiles* documentation.

2 Select the host profile and click **Edit Host Profile**.

3 Leave the name and description and click **Next**.

4 Click **Advanced Configuration Settings** and click the **System Image Cache Configuration** folder.

5 Click the **System Image Cache Configuration** icon.

6 In the System Image Cache Profile Settings drop-down menu, make your selection.

Option	Description
Enable stateless caching on the host	Caches the image to disk.
Enable stateless caching to a USB disk on the host	Caches the image to a USB disk attached to the host.

7 If you selected **Enable stateless caching on the host**, specify information about the disk to use.

Option	Description
Arguments for first disk	By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use **`esx`** for the first disk with ESX installed on it, use model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that uses the mptsas driver, and third for the local disk, specify **`ST3120814A,mptsas,local`** as the value of this field.
Check to overwrite any VMFS volumes on the selected disk	If you click this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.

8 Click **Finish** to complete the host profile configuration.

9 Apply the host profile with the vSphere Client, the vSphere Web Client, or the vSphere PowerCLI.

Option	Description
vSphere Client or vSphere Web Client	Use the host profiles interface of the vSphere Client or the vSphere Web Client. See the *Host Profiles* documentation.
vSphere PowerCLI	See "Assign a Host Profile to Hosts," on page 83.

Enable Stateful Installs for Hosts Provisioned with Auto Deploy

You can set up hosts provisioned with Auto Deploy to cache the image to disk and to use the cached image on subsequent boots. After the image is cached, the hosts act like hosts on which an image is installed.

Prepare Hosts Provisioned with Auto Deploy for Stateful Installs

In some situations, it is useful to provision hosts with Auto Deploy and to perform all subsequent boots from disk. This approach is called Stateful Installs.

Prerequisites

Decide which disk to use for storing the image, and determine whether the new image will overwrite an existing VMFS partition.

Procedure

1 Set up your environment for Auto Deploy and install PowerCLI.

See "Preparing for vSphere Auto Deploy," on page 75.

2 Verify that a disk with at least 1GB of free space is available.

If the disk is not partitioned, partitioning happens when you apply the host profile.

3 Set up the host to boot from disk.

See your hardware vendor's documentation.

Configure a Host Profile to Enable Stateful Installs

To set up a host provisioned with Auto Deploy to boot from disk, you must configure a host profile. You can apply that host profile to other hosts that you want to set up for stateful installs.

You can configure the host profile on a single host. You can also create a host profile on a reference host and apply that host profile to other hosts.

Prerequisites

Make sure that your host is configured for Auto Deploy and that you meet other prerequisites for stateful installs. See "Prepare Hosts Provisioned with Auto Deploy for Stateful Installs," on page 95.

Procedure

1 In the vSphere Web Client, create a host profile.

See the *Host Profiles* documentation.

2 With the host profile object displayed, click the Edit host profile settings icon.

3 Leave the name and description and click **Next**.

4 Click **Advanced Configuration Settings** and click the **System Image Cache Configuration** folder.

5 Click the **System Image Cache Configuration** icon.

6 In the System Image Cache Profile Settings drop-down menu, make your selection.

Option	Description
Enable stateful installs on the host	Caches the image to a disk.
Enable stateful installs to a USB disk on the host	Caches the image to a USB disk attached to the host.

7 If you select **Enable stateful installs on the host**, specify information about the disk to use.

Option	Description
Arguments for first disk	By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use **`esx`** for the first disk with ESX installed on it, use model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that uses the mptsas driver, and third for the local disk, specify **`ST3120814A,mptsas,local`** as the value of this field.
Check to overwrite any VMFS volumes on the selected disk	If you click this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.

8 Click **Finish** to complete the host profile configuration.

9 Apply the host profile with the vSphere Client, the vSphere Web Client, or the vSphere PowerCLI.

Option	Description
vSphere Client or vSphere Web Client	To apply the host profile to individual hosts, use the host profiles interface of the vSphere Client or the vSphere Web Client. See the *Host Profiles* documentation.
vSphere PowerCLI	To apply the host profile to one or more hosts by using PowerCLI, see "Assign a Host Profile to Hosts," on page 83.

Setting Up an Auto Deploy Reference Host

In an environment where no state is stored on the host, a reference host helps you set up multiple hosts with the same configuration. You configure the reference host with the logging, coredump, and other settings that you want, save the host profile, and write a rule that applies the host profile to other hosts as needed.

You can configure the storage, networking, and security settings on the reference host and set up services such as syslog and NTP.

Understanding Reference Host Setup

A well-designed reference host connects to all services such as syslog, NTP, and so on. The reference host might also include setup of security, storage, networking, and ESXi Dump Collector. You can then apply the host setup to other hosts with host profiles.

The exact setup of your reference host depends on your environment, but you might consider the following customization.

NTP Server Setup

When you collect logging information in large environments, you must make sure that log times are coordinated. Set up the reference host to use the NTP server in your environment that all hosts can share. You can specify an NTP server with the `vicfg-ntp` command. You can start and stop the NTP service for a host with the `vicfg-ntp` command, the vSphere Client, or the vSphere Web Client.

Syslog Server Setup

All ESXi hosts run a syslog service (`vmsyslogd`), which logs messages from the VMkernel and other system components to a file. You can specify the log host and manage the log location, rotation, size, and other attributes with the `esxcli system syslog` vCLI command or with the vSphere Web Client. Setting up logging on a remote host is especially important for hosts provisioned with Auto Deploy that have no local storage. You can optionally install the vSphere Syslog Collector to collect logs from all hosts.

Core Dump Setup

You can set up your reference host to send core dumps to a shared SAN LUN, or you can install ESXi Dump Collector in your environment and set up the reference host to use ESXi Dump Collector. See "Configure ESXi Dump Collector with ESXCLI," on page 99. You can either install ESXi Dump Collector by using the vCenter Server installation media or use the ESXi Dump Collector that is included in the vCenter Server Appliance. After setup is complete, VMkernel memory is sent to the specified network server when the system encounters a critical failure.

Security Setup

In most deployments, all hosts that you provision with Auto Deploy must have the same security settings. Make any customization in your reference host. You can, for example, set up the firewall to allow certain services access to the ESXi system. See the *vSphere Security* documentation. Security setup includes shared user access settings for all hosts. You can achieve unified user access by setting up your reference host for Microsoft Active Directory.

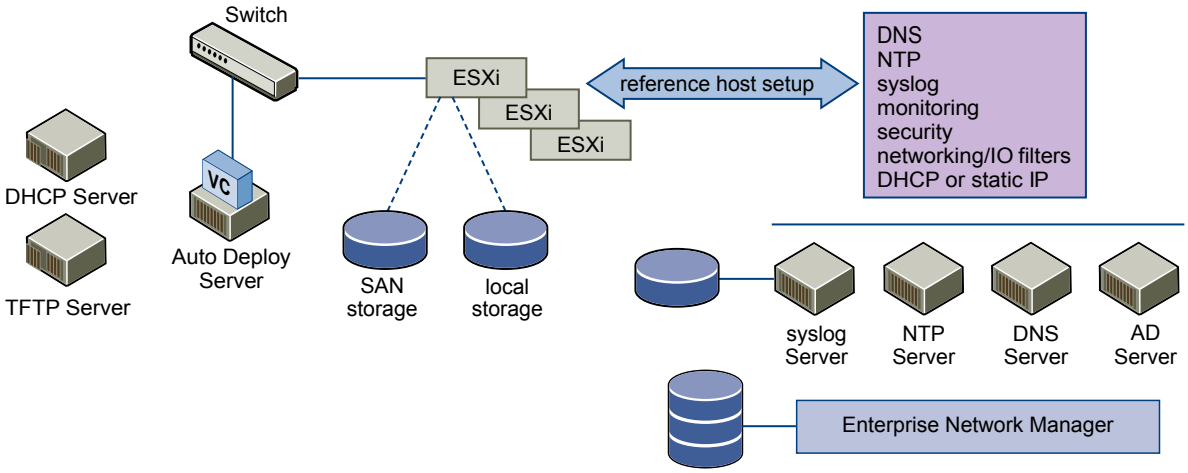
NOTE If you set up Active Directory by using host profiles, the passwords are not protected. Use the vSphere Authentication Service to set up Active Directory to avoid exposing the Active Directory password.

Networking and Storage Setup

If you reserve a set of networking and storage resources for use by hosts provisioned with Auto Deploy, you can set up your reference host to use those resources.

In very large deployments, the reference host setup supports an Enterprise Network Manager, which collects all information coming from the different monitoring services in the environment.

Figure 5-4. Auto Deploy Reference Host Setup



"Configuring an Auto Deploy Reference Host," on page 98 explains how to perform this setup.

Configuring an Auto Deploy Reference Host

vSphere allows you to configure a reference host by using the vSphere Web Client or the vSphere Client, by using vCLI, or by using host profiles.

To set up a host profile, you can use the approach that suits you best.

vSphere Web Client and vSphere Client

The vSphere Web Client and vSphere Client support setup of networking, storage, security, and most other aspects of an ESXi host. You can completely set up your environment in the reference and create a host profile from the reference host for use by Auto Deploy.

vSphere Command-Line Interface

You can use vCLI commands for setup of many aspects of your host. vCLI is especially suitable for configuring some of the services in the vSphere environment. Commands include `vicfg-ntp` (set up an NTP server), `esxcli system syslog` (set up a syslog server), and `esxcli network route` (add routes and set up the default route). See "Configure ESXi Dump Collector with ESXCLI," on page 99.

Host Profiles Interface

Best practice is to set up a host with vSphere Web Client, vSphere Client, or vCLI and create a host profile from that host. You can also configure the host profiles directly with the Host Profiles interface in the vSphere Web Client or the vSphere Client. See "Configure Host Profiles for an Auto Deploy Reference Host in the vSphere Client," on page 99 and "Configure Host Profiles for an Auto Deploy Reference Host with the vSphere Web Client," on page 102.

Configure ESXi Dump Collector with ESXCLI

A core dump is the state of working memory in the event of host failure. By default, a core dump is saved to the local disk. You can use ESXi Dump Collector to keep core dumps on a network server for use during debugging. ESXi Dump Collector is especially useful for Auto Deploy, but is supported for any ESXi host. ESXi Dump Collector supports other customization, including sending core dumps to the local disk.

Prerequisites

Install ESXi Dump Collector, a support tool that is included with the vCenter Server `autorun.exe` application and that is also included in the vCenter Server Appliance.

Install vCLI if you want to configure the host to use ESXi Dump Collector. In troubleshooting situations, you can use ESXCLI in the ESXi Shell instead.

Procedure

1 Set up an ESXi system to use ESXi Dump Collector by running `esxcli system coredump` in the local ESXi Shell or by using vCLI.

```
esxcli system coredump network set --interface-name vmk0 --server-ipv4 10xx.xx.xx.xx --server-port 6500
```

You must specify a VMkernel NIC and the IP address and optional port of the server to send the core dumps to. If you configure an ESXi system that is running inside a virtual machine that is using a vSphere standard switch, you must choose a VMkernel port that is in promiscuous mode. ESXi Dump Collector is not supported on vSphere distributed switches.

2 Enable ESXi Dump Collector.

```
esxcli system coredump network set --enable true
```

3 (Optional) Check that ESXi Dump Collector is configured correctly.

```
esxcli system coredump network check
```

The host on which you have set up ESXi Dump Collector is set up to send core dumps to the specified server by using the specified VMkernel NIC and optional port.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83).
- For hosts that are already provisioned with Auto Deploy, perform the test and repair compliance operations to provision them with the new host profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new host profile.

Configure Host Profiles for an Auto Deploy Reference Host in the vSphere Client

You can set up host profiles in a reference host and apply those host profile settings to all other hosts that you provision with vSphere Auto Deploy. You can either configure the reference host and export the host profile or, for small changes, edit the reference host's host profiles directly and export the host profile.

Prerequisites

Install a vSphere Client to access the vCenter Server system that manages the host that you want to use as a reference host.

Procedure

1 Use a vSphere Client to connect to the vCenter Server system.

2 Select the host and select **View > Management > Host Profiles**.

3 For a new profile, click **Create Profile**, or right-click a profile that you want to modify and select **Edit Profile**.

4 In the Edit Profile dialog, select the fields for the policy that you want to set up.

Policy	Description
ESXi Dump Collector	Set up ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (best practice), or configure the host profile directly. See "Set Up ESXi Dump Collector from the Host Profiles Interface in the vSphere Client," on page 100.
Syslog	Set up syslog for the host with the `esxcli system syslog` command. Save the host profile (best practice) or configure the host profile directly. See "Set Up Syslog from the Host Profiles Interface in the vSphere Client," on page 101.
NTP	Use the `vicfg-ntp` vCLI command or the vSphere Client to set up a host. If you use the vSphere Client to start the NTP Server, make sure the startup policy for the NTP Daemon is set appropriately. a In the vSphere Client, select the **Configuration** tab and click **Time Configuration** in the Software panel. b Click **Properties**, click the NTP Client Enabled check box and click **Options**. c Select the **Start and stop with host** button.
Security	Set up the firewall configuration, security configuration, user configuration, and user group configuration for the reference host with the vSphere Client or with vCLI commands.
Networking and Storage	Set up the networking and storage policies for the reference host with the vSphere Client or vCLI command.

5 Click **OK** to save the host profile settings.

What to do next

Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83), and perform a test and repair compliance operation.

Set Up ESXi Dump Collector from the Host Profiles Interface in the vSphere Client

You can set up ESXi Dump Collector for a reference host with `esxcli` or directly in the Host Profiles panels of the vSphere Client. You can export the host profile and write a rule that applies the profile to all hosts provisioned with Auto Deploy.

Best practice is to set up hosts to use ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (see "Configure ESXi Dump Collector with ESXCLI," on page 99). If you prefer using a GUI, setting up ESXi Dump Collector from the Host Profiles interface is an alternative.

Prerequisites

You must have a partition that has sufficient storage capability for core dumps from multiple hosts provisioned with vSphere Auto Deploy.

Procedure

1 Use a vSphere Client to connect to the vCenter Server system.

2 Select the host and select **View > Management > Host Profiles**.

3 For a new profile, click **Create Profile**, or right-click a profile you want to modify and select **Edit Profile**.

4 Select **Network Configuration**.

5 Select **Network Coredump Settings** and click **Edit**.

6 Specify the server port and IP address and the host NIC to use and click the check box to enable ESXi Dump Collector.

7 Click **OK** to save the host profile settings.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83).
- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new host profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new host profile.

Set Up Syslog from the Host Profiles Interface in the vSphere Client

Hosts provisioned with Auto Deploy usually do not have sufficient local storage to save system logs. You can specify a remote syslog server for those hosts by setting up a reference host, saving the host profile, and applying that host profile to other hosts as needed.

Best practice is to set up the syslog server on the reference host with the vSphere Client or the `esxcli system syslog` command and save the host profile. In some situations, setting up syslog from the Host Profiles interface is an alternative.

Prerequisites

If you intend to use a remote syslog host, set up that host before you customize host profiles.

Procedure

1 Use a vSphere Client to connect to the vCenter Server system.

2 Select the host and select **View > Management > Host Profiles**.

3 (Optional) Click **Create Profile** if no reference host exists in your environment.

4 Right-click the profile to modify and select **Edit Host Profile**.

System	Description
ESXi 5.0, no previously configured syslog server	a Right-click **Advanced configuration option** and select **Add Profile**. b Open the Advanced configuration option folder and scroll to the bottom. c Click **Option Profile**, click **Edit**, and select **Configure a fixed option**. d Specify `Syslog.global.logHost` as the option name and the name or IP address of the syslog server as the option value. You must specify a valid syslog server or you cannot save the host profile policy.
ESXi 5.1, or ESXi 5.0 with previously configured syslog server	a Select **Advanced configuration option**. b Select Syslog.global.loghost to specify the host, and specify other settings that you want to use.

5 Click **OK** to save the host profile settings.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83).

- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new image profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new image profile.

Set Up Networking for Your Auto Deploy Host

You can set up networking for your Auto Deploy reference host and apply the host profile to all other hosts to guarantee a fully functional networking environment.

Prerequisites

Provision the host you wish to use as your reference host with an ESXi image by using Auto Deploy.

Procedure

1 In the vSphere Client select **Configuration**, click **Networking** in the Hardware panel, and verify that vmk0 is connected to the Management Network.

2 If you are using virtual switches and not vSphere Distributed Switch, do not add other VMkernel NICs to vSwitch0.

3 After the reference host is completely configured, reboot the system to verify that vmk0 is connected to the Management Network.

4 Export the host profile.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83).
- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new host profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new host profile.

Configure Host Profiles for an Auto Deploy Reference Host with the vSphere Web Client

You can set up host profiles in a reference host and apply the host profile settings to all other hosts that you provision with vSphere Auto Deploy. You can either configure the reference host and export the host profile or, for small changes, edit the host profiles directly.

Prerequisites

Verify that you have access to a vSphere Web client that can connect to the vCenter Server system

Procedure

1 In the vSphere Web Client, click **Rules and Profiles** and click **Host Profiles**.

2 For a new profile, click the **Create Profile from a host** icon, or right-click a profile that you want to modify and select **Edit Host Profile**.

3 Customize your reference host by using vCLI, by using the client UI, or by using the Host Profiles interface.

Policy	Description
ESXi Dump Collector	Set up ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (best practice), or configure the host profile directly. See "Set Up Syslog from the Host Profiles Interface in the vSphere Web Client," on page 104.
Syslog	Set up syslog for the host with the `esxcli system syslog` command. Save the host profile (best practice) or configure the host profile directly. See "Set Up Syslog from the Host Profiles Interface in the vSphere Web Client," on page 104.
NTP	Use the `vicfg-ntp` vCLI command or the vSphere Web Client to set up a host. If you use the vSphere Web Client to start the NTP Server, make sure the startup policy for the NTP Daemon is set appropriately. a In the vSphere Web Client, select the host. b Select the Manage tab and click **Time Configuration**. c Click **Edit** and click Use Network Time Protocol (Enable NTP client). d Select **Start and stop with host** as the NTP Service Startup Policy.
Security	Set up the firewall configuration, security configuration, user configuration, and user group configuration for the reference host with the vSphere Web Client or with vCLI commands. See the *vSphere Security* documentation.
Networking and Storage	Set up the networking and storage policies for the reference host with the vSphere Web Client or vCLI command.

4 Click **OK** to save the host profile settings.

What to do next

Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83). Perform a test-and-repair compliance operation.

Set Up ESXi Dump Collector from the Host Profiles Interface in the vSphere Web Client

You can set up ESXi Dump Collector for a reference host with `esxcli` or directly in the Host Profiles panels of the vSphere Web Client. You can export the host profile and write a rule that applies the profile to all hosts provisioned with Auto Deploy.

Best practice is to set up hosts to use ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (see "Configure ESXi Dump Collector with ESXCLI," on page 99). If you prefer to use a GUI, set up ESXi Dump Collector from the Host Profiles interface.

Prerequisites

Verify that at least one partition has sufficient storage capability for core dumps from multiple hosts provisioned with vSphere Auto Deploy.

Procedure

1 In the vSphere Web Client, click **Rules and Profiles** and click **Host Profiles**.

2 For a new profile, click the **Create Profile from a host** icon, or right-click a profile that you want to modify and select **Edit Host Profile**.

3 Leave the name and description and click **Next**.

4 Select **Network Configuration**.

5 Select **Network Coredump Settings**.

6 Click the **Enabled** check box.

7 Specify the host NIC to use, the Network Coredump Server IP, and the Network Coredump Server Port.

8 Click **Finish** to save the host profile settings.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host. See "Assign a Host Profile to Hosts," on page 83.
- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new host profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new host profile.

Set Up Syslog from the Host Profiles Interface in the vSphere Web Client

Hosts provisioned with Auto Deploy usually do not have sufficient local storage to save system logs. You can specify a remote syslog server for those hosts by setting up a reference host, saving the host profile, and applying that host profile to other hosts as needed.

Best practice is to set up the syslog server on the reference host with the vSphere Web Client or the `esxcli system syslog` command and to save the host profile. You can also set up syslog from the Host Profiles interface.

Prerequisites

- If you intend to use a remote syslog host, set up that host before you customize host profiles.
- Verify that you have access to a vSphere Web Client that can connect to the vCenter Server system.

Procedure

1 In the vSphere Web Client, click **Rules and Profiles** and click **Host Profiles**.

2 (Optional) If no reference host exists in your environment, click the **Extract Profile from Host** icon to create a host profile.

3 Right-click the host profile you want to modify and select **Edit Host Profile**.

4 Leave the name and description and click **Next**.

5 Click **Advanced Configuration Settings** click the **Advanced Options** folder, and click **Advanced configuration options**.

You can specify syslog settings from here.

6 If you are setting up an ESXi 5.0 host that did not have a previously configured syslog server, you have to create an advanced configuration option.

a Click the plus sign.

b Click the new Advanced configuration option at the top of the option list and select **Configure a fixed option** from the drop-down menu.

c Specify Syslog.global.loghost as the option, and your host as the value.

If you are configuring an ESXi 5.1 host or an ESXi 5.0 host that has syslog configured, Syslog.global.loghost is already in the list of advanced options.

7 Click **OK** to save the host profile settings.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Assign a Host Profile to Hosts," on page 83).

- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new image profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new image profile.

Set Up Networking for Your Auto Deploy Host in the vSphere Web Client

You can set up networking for your Auto Deploy reference host and apply the host profile to all other hosts to guarantee a fully functional networking environment.

Prerequisites

Provision the host you want to use as your reference host with an ESXi image by using Auto Deploy.

Procedure

1 In the vSphere Web Client, select the host and click the **Networking** tab.

2 Perform networking setup.

If you are using virtual switches and not vSphere Distributed Switch, do not add other VMkernel NICs to vSwitch0.

3 After the reference host is configured, reboot the system to verify that vmk0 is connected to the Management Network.

4 Create a host profile from the host.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host. See "Assign a Host Profile to Hosts," on page 83.
- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new host profile. See "Test and Repair Rule Compliance," on page 85.
- Turn on unprovisioned hosts to provision them with the new host profile.

Consider and Implement Your Partitioning Stategy

By default, Auto Deploy provisions hosts only if a partition is available on the host. You can set up a reference host to auto-partition all hosts that you provision with Auto Deploy.

CAUTION If you change the default auto-partitioning behavior, Auto Deploy overwrites existing partitions regardless of their content. If you turn on this option, ensure that no unintended data loss results.

Prerequisites

- Provision the host you wish to use as your reference host with an ESXi image by using Auto Deploy.
- Verify that you have access to a vSphere Web Client that can connect to the vCenter Server system.

Procedure

1 In the vSphere Web Client, select the host you want to use as a reference host and click **Manage**.

2 Click **Settings**.

3 Click **System** to open the system options and click **Advanced System Settings**.

4 Scroll to VMkernel.Boot.autoPartition and set the value to true.

5 If no host profile exists for your reference host, create it now.

6 Use the Auto Deploy PowerCLI to write a rule that applies the host profile of your reference host to all hosts immediately when they boot.

Auto-partitioning is performed when the hosts boot.

Advanced Management Tasks

In most cases, you manage your Auto Deploy environment by preparing system setup, writing rules, and provisioning hosts. In some cases, you might perform advanced management tasks such as reregistering the Auto Deploy server or assigning a static IP address to each host.

Reregister Auto Deploy

If the IP address of the vCenter Server changes, you must reregister Auto Deploy.

Regardless of whether you are using the vCenter Server Appliance or a vCenter Server system installed on Windows, you must stop the Auto Deploy process and reregister Auto Deploy if the vCenter Server IP address changes.

Procedure

- Perform the reregistration task depending on the operating system.

Platform	Task

Windows	a Stop the Auto Deploy process.
	`net stop vmware-autodeploy-waiter`
	b Edit the setup file located at `c:\ProgramData\VMware\VMware vCenter Auto Deploy\vmconfig-autodeploy.xml` and specify the new IP address.
	You do not have to edit the file if you reregister for other reasons than a new IP address.
	c Run the `autodeploy-register.exe` command, specifying all required options.
	`autodeploy-register.exe -R -a vCenter-IP -p vCenter-Port -u user_name -w password -s setup-file-path`
	d Restart the Auto Deploy process.
	`net start vmware-autodeploy-waiter`

VMware vCenter Server Appliance	a Stop the Auto Deploy process.
	`/etc/init.d/vmware-rbd-watchdog stop`
	b Run the `autodeploy-register` command, specifying all required options.
	`autodeploy-register -R -a vCenter-IP -p vCenter-Port -u user_name -w password -s setup-file-path`
	c Restart the Auto Deploy process.
	`/etc/init.d/vmware-rbd-watchdog start`
	You can also use the **Start ESXi Services** and **Stop ESXi Services** buttons in the vCenter Server Appliance.

Set Up Host Profiles for Static IP Addresses in the vSphere Client

By default, hosts provisioned with Auto Deploy are assigned DHCP addresses by a DHCP server. You can use the Auto Deploy answer file mechanism to assign static IP addresses to hosts.

You can configure your DHCP server to return a fixed IP address for each machine's MAC address so that the IP address is consistent across boots. See your DHCP server documentation for more information.

Prerequisites

Set up your Auto Deploy environment.

Procedure

1 Boot a host using Auto Deploy.

2 With vSphere Client connect to the vCenter Server that manages the Auto Deploy host, select the host, and select **View > Management > Host Profiles** to display the host profile.

3 Select a host, select **Edit Profile**, and select **Networking configuration > Host port group > Management Network > IP address settings > IP address**.

4 Select **User specified IP address to be used while applying the configuration**.

5 Select **Networking configuration > DNS configuration > DNS settings** and make sure the **Flag indicating if DHCP should be used** check box is not selected.

6 If the host is in a different subnet than the vCenter Server system, select **Network Configuration > IP route configuration > Default gateway for IPv4 routing > Default IPv4 gateway**and supply the default route.

7 Export the host profile and modify the rule that assigns a host profile to the hosts for which you want to use a static IP address.

8 In the vSphere Client, apply the host profile to be prompted for the information without rebooting.

   a Right-click the host, select **Host Profiles > Manage Profile**, select the profile to attach, and click **OK**.

   b Right-click the host and select **Enter Maintenance Mode**.

   c Right-click the host and select **Host Profiles > Apply Profile**.

   d When prompted, provide the IP address.

   e Right-click the host and select **Exit Maintenance Mode**.

The IP address 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.

Set Up Host Profiles for Static IP Addresses in the vSphere Web Client

By default, hosts provisioned with Auto Deploy are assigned DHCP addresses by a DHCP server. You can use the Auto Deploy host customization mechanism to assign static IP addresses to hosts.

Prerequisites

- Set up your Auto Deploy environment.
- Boot the host using Auto Deploy.
- Extract a host profile from the host.

Procedure

1 With vSphere Web Client, connect to the vCenter Server that manages the Auto Deploy host, select **Rules and Profiles**, and select **Host Profiles**.

2 Right-click the host profile you just extracted and click **Edit Host Profile**.

3 Use the default name and description and click **Next**.

4 Follow these steps to change the default IP address settings.

   a Click **Networking configuration**.

   b Click **Host port group**.

c Click **Management Network**.

d Click**IP address settings**

5 From the IPv4 address drop-down menu, select **User specified IP address to be used while applying the configuration**.

6 If the host is in a different subnet than the vCenter Server system, select **Network Configuration > IP route configuration > IP route config**and supply the default route in the Default IPv4 gateway field.

7 Select **Networking configuration** and click **DNS configuration**. In the DNS settings field, make sure the **Flag indicating if DHCP should be used** check box is not selected.

8 Remediate the host to update the host customization information.

a Right-click the host, select **All vCenter Actions > Host Profiles > Attach Host Profile**, select the profile to attach, and click **OK**.

b Right-click the host and select **Enter Maintenance Mode**.

c Right-click the host and select **All vCenter Actions > Host Profiles > Remediate**.

d When prompted, provide the IP address.

e Right-click the host and select **Exit Maintenance Mode**.

The IP address is saved as a host customization. The next time you boot, the host customization information is applied to the host.

Using Auto Deploy with the VMware vCenter Server Appliance

The VMware vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services. The appliance includes an Auto Deploy server that is disabled by default.

You can use Auto Deploy with the vCenter Server Appliance in different ways.

- Use the vCenter Server system on the appliance in conjunction with the Auto Deploy server on the appliance.
- Use the vCenter Server system on the appliance in conjunction with an Auto Deploy server that you install separately on a Windows system.
- Use the Auto Deploy server on the appliance in conjunction with a vCenter Server system that you install on a different vCenter Server Appliance.
- Use the Auto Deploy server on the appliance in conjunction with a vCenter Server system that you install separately on a Windows system.

NOTE If you want to use the Auto Deploy server on the vCenter Server Appliance, you must start the service first. You can start the service from the Summary tab of the appliance.

In all cases, you are responsible for setting up your DHCP server. See "Prepare Your System and Install the Auto Deploy Server," on page 76.

NOTE You can register only one Auto Deploy instance with a vCenter Server system, and only one vCenter Server system with an Auto Deploy server.

You can set up a mixed-mode environment that includes an IPv6 vCenter Server. The Auto Deploy server must have an IPv4 address because PXE booting is supported only with IPv4.

Set Up the vCenter Server Appliance to Use a Standalone Auto Deploy Server

The vCenter Server Appliance includes an Auto Deploy server. You can also use the appliance with a standalone Auto Deploy server.

Prerequisites

- Deploy the vCenter Server Appliance.
- Obtain the vCenter Server installation media, which include the Auto Deploy installer.
- Verify that the Windows system that you want to use for Auto Deploy meets the requirements for vCenter Server installation. Auto Deploy has the same requirements.

Procedure

1 If Auto Deploy is running on the vCenter Server Appliance, stop the built-in Auto Deploy server and unregister Auto Deploy from the Linux command prompt.

```
service vmware-rdb-watchdog stop
autodeploy-register --unregister -a localhost -l
```

If you never started Auto Deploy on the appliance, this step is not necessary.

2 Using the vCenter Server installation media, install Auto Deploy on a Windows system and provide the vCenter Server Appliance information when prompted for the vCenter Server.

Your standalone Auto Deploy installation is now associated with the vCenter Server on the vCenter Server Appliance.

Set Up Auto Deploy on the vCenter Server Appliance

By default, Auto Deploy on the vCenter Server Appliance is preconfigured to use the vCenter Server system running on the appliance. You can set up Auto Deploy to use a different vCenter Server system.

Prerequisites

- Deploy the vCenter Server Appliance.
- Install a vCenter Server system to use with Auto Deploy.

Procedure

1 If Auto Deploy is running on the vCenter Server Appliance, stop the built-in Auto Deploy server and unregister Auto Deploy from the Linux command prompt.

```
service vmware-rdb-watchdog stop
autodeploy-register --unregister -a localhost -l
```

If you never started Auto Deploy on the appliance, this step is not necessary.

By default, the Auto Deploy daemon is not running.

2 The next step depends on whether you want to confirm the vCenter Server thumbprint while registering.

- Register and pass in a thumbprint that you created earlier as part of the registration.

```
autodeploy-register --register -a vcenter-ip -u username -w password-R -T thumbprint
```

- Register without using a thumbprint.

```
autodeploy-register --register -a vcenter-ip -u username -w password -R
```

3 Restart the Auto Deploy daemon

```
service vmware-rbd-watchdog restart
```

Customizing Hosts with Answer Files in the vSphere Client

To customize hosts with shared attributes, you can create a host profile in a reference host. To customize each host with a different value, you can set up some fields in the host profile to prompt the user for input for each host. After the user has specified the information, the system generates a host-specific answer file and stores it with the Auto Deploy cache and the vCenter Server host object.

Host profiles allow you to prespecify information, for example, the storage setup or Syslog setup in a reference host and apply the host profile to a set of target hosts that share the same settings. You can also use host profiles to specify that certain settings are host-dependent. If you do so, the host comes up in maintenance mode when you provision it with Auto Deploy. Apply the host profile or update the answer file to be prompted for input. The system stores your input and uses it the next time the host boots.

NOTE The answer file is not stored in a location or format that administrators can access. Use the Host Profiles UI in the vSphere Client to manage answer files.

When the host profile is set to prompt for user input, you must specify a value in the dialog that appears. An error results if you do not specify a value.

Table 5-7. Host Profile Options for iSCSI

Information to Request User Input For		Setting the Host Profile Option
When you apply a host profile on a system that includes a profile for iSCSI, you are prompted for several properties. For many of the properties, a system default is available. For some properties, you must specify a value or an error results.		1 Select **Storage configuration** and click **iSCSI Initiator Configuration** 2 If the HBA you want to configure is not in the list, Right-click the folder that corresponds to the initiator you want to configure and select **Add Profile**. You have to add a profile, for example, if software iSCSI was not enabled during host profile creation and you want to configure the software iSCSI initiator. 3 Set up the initiator. For many fields, the user is prompted when you apply the profile.
IQN name	If the iSCSI setup uses an IQN name, you are prompted when you apply the host profile. You cannot continue until you provide the name.	
CHAP information	If you set up iSCSI to require CHAP authentication, you are prompted for CHAP information including the user name and the secret when you apply the host profile. You cannot continue until you provide the name.	

Table 5-8. Host Profile Options that Prompt for Storage User Input

Information to Request User Input For	Setting the Host Profile Option
You are setting up the Fixed PSP configuration and want to prompt for the adapter and target IDs for the storage arrays that should use the Fixed PSP.	1 Create a subprofile. a Click **Storage configuration**. b Click **Native Multipathing (NMP)**. c Click **Path Selection Policy (PSP) configuration**. d Right-click **Fixed PSP Configuration** and select **Add Profile**. 2 In the profile's Preferred Path window, select **Prompt the user for adapter and target IDs on the host**.
Configure FCoE adapter activation based on a user-specified MAC address.	1 Open **Storage configuration**. 2 Open **Software FCoE configuration**. 3 Open **Adapter Configuration**. 4 If no activation profile exists, right-click **Activation Profile** and select **New Profile**. 5 Open the profile and click **Policy Profile**. 6 Select **Activation policy based on adapter MAC address** from the drop-down menu.

Table 5-9. Host Profile Options that Prompt for Security User Input

Information to Request User Input For	Setting the Host Profile Option
Administrator password for ESXi host when the host boots for the first time.	1 Open **Security configuration**. 2 Click **Administrator password**. 3 Select **User Input Password to be Used to Configure Administrator Password**.
Preconfigures a user for the ESXi host but prompts for the password for that user on each host when the host boots for the first time.	1 Create a user profile by right-clicking User Configuration and selecting **Add Profile**. 2 Configure the user by selecting one of the options. ■ **Assigned fixed user configurations** is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear. ■ **Assign advanced fixed user configurations** is for users of ESXi 5.0 systems. ■ **Specify the user configuration in the profile but prompt for password during host configuration** allows you to specify the information about the user but prompt for a password on each host.
Prompt the user for credentials when the host joins the Active Directory domain.	1 Set the Authentication configuration profile to use a fixed domain. a Open **Authentication configuration**. b Open **Active Directory configuration**. c Click **Domain Name**. d Select **Configure a fixed domain name**. 2 Set the method for joining the domain to prompt the user. a Open **Authentication configuration**. b Open **Active Directory configuration**. c Click **JoinDomain Method**. d Select **Use user specified AD credentials to join the host to domain**.

Table 5-10. Host Profile Options that Prompt for Networking User Input

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the MAC address for a port group. You can have the system prompt the user in all cases (User specified MAC address...) or prompt the user only if no default is available.	1 Open **Networking configuration**. 2 Open **Host port group**. 3 Open **Management Network**. 4 Click **Determine how MAC address for vmknic should be decided**. 5 Select how the system manages the MAC address. ■ **User specified MAC Address to be used while applying the configuration** ■ **Prompt the user for the MAC Address if no default is available**
Prompt the user for the IPv4 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv4 address...) or prompt the user only if no default is available.	1 Open **Networking configuration**. 2 Open **Host port group**. 3 Open **Management Network**. 4 Open **IP address settings**. 5 Click **IPv4 address**. 6 Select how the system manages the IPv4 address. ■ **User specified IPv4 address to be used while applying the configuration** ■ **Prompt the user for the IPv4 address if no default is available**
Prompt the user for the IPv6 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv6 address...) or prompt the user only if no default is available.	1 Open **Networking configuration**. 2 Open **Host port group**. 3 Open **Management Network**. 4 Open **IP address settings**. 5 Click **Static IPv6 address**. 6 Select how the system manages the IPv6 address. ■ **User specified IPv6 address to be used while applying the configuration** ■ **Prompt the user for the IPv6 address if no default is available**
Prompt the user for the DNS name of the host. You can have the system prompt the user in all cases (User specified host name...) or prompt the user only if no default is available.	1 Open **Networking configuration**. 2 Open **DNS configuration**. 3 In the right panel, click **Edit** next to What is the name of this host. 4 Select how the system manages the DNS configuration. ■ **Prompt the user for host name if default is not available** ■ **User specified host name to be used while applying the configuration**
Prompt the user for the MAC address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click **Add profile** to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Open **Host virtual NIC**. 3 Open *dvSwitch*:*dvPortGroup* The available port group depends on your environment. 4 Click **Determine how MAC address for vmknic should be decided**. 5 Select how the system manages the MAC address for the distributed switch. ■ **User specified MAC address to be used while applying the configuration** ■ **Prompt the user for the MAC address if no default is available**

Table 5-10. Host Profile Options that Prompt for Networking User Input (Continued)

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the IPv4 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click **Add profile** to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Open **Host virtual NIC**. 3 Open *dvSwitch*:*dvPortGroup* The available port group depends on your environment. 4 Open **IP address settings**. 5 Click **IPv4 address**. 6 Select how the system handles the IPv4 address for the distributed switch. ■ **User specified IPv4 address to be used while applying the configuration** ■ **Prompt the user for IPv4 address if no default is available**
Prompt the user for the IPv6 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click **Add profile** to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Open **Host virtual NIC**. 3 Open *dvSwitch*:*dvPortGroup* The available port group depends on your environment. 4 Open **IP address settings**. 5 Click **Static IPv6 address**. 6 Select how the system manages the IPv6 address for the distributed switch. ■ **User specified IPv6 address to be used while applying the configuration** ■ **Prompt the user for IPv6 address if no default is available**

Host Customization in the vSphere Web Client

To customize hosts with shared attributes, you can create a host profile in a reference host. To customize individual hosts, you can set up some fields in the host profile to prompt the user for input for each host.

Host profiles allow you to prespecify information, for example, the storage setup or Syslog setup in a reference host to and apply the host profile to a set of target hosts that share the same settings. You can also use host profiles to specify that certain settings are host dependent. If you do so, the host comes up in maintenance mode when you provision it with Auto Deploy. Remediate the host or reset the host customization to be prompted for input. The system stores your input and uses it the next time the host boots.

NOTE The host customization is not stored in a location or format that administrators can access. Use the Host Profiles UI in the vSphere Web Client to modify customization.

When the host profile is set to prompt for user input, you must specify a value in the dialog that appears when you reset the host customization. An error results if you do not specify a value.

Table 5-11. Host Profile Options that Prompt for iSCSI User Input

Information to Request User Input For		Setting the Host Profile Option
When you apply a host profile on a system that includes a profile for iSCSI, you are prompted for several properties. For many of the properties, a system default is available. For some properties, you must specify a value or an error results.		1 Select **Edit Host Profile**, click **Storage configuration**, and click **iSCSI Initiator Configuration**. 2 Select the folder for an already enabled initiator and set up the initiator. 3 Set up the initiator. For many fields, the user is prompted as part of host customization.
IQN name	If the iSCSI setup uses an IQN name, you are prompted when you apply the host profile. You cannot continue until you provide the name.	
CHAP information	If you set up iSCSI to require CHAP authentication, you are prompted for CHAP information including the user name and the secret when you apply the host profile. You cannot continue until you provide the name.	

Table 5-12. Host Profile Options that Prompt for Storage User Input

Information to Request User Input For	Setting the Host Profile Option
You are setting up the Fixed PSP configuration and want to prompt for the adapter and target IDs for the storage arrays that should use the Fixed PSP.	You can set the option only if the adapter is set up to use the Fixed PSP. 1 Select **Edit Host Profile**, click **Storage configuration**. 2 Click **Native Multipathing (NMP)**. 3 Click **Path Selection Policy (PSP) configuration**. 4 In the Preferred Path window, select **Prompt the user for adapter and target IDs on the host**.
Configure FCoE adapter activation based on a user-specified MAC address.	You can set the option only if an activation profile exists. 1 Select **Edit Host Profile**, click **Storage configuration**. 2 Click **Software FCoE configuration**. 3 Click **Adapter Configuration**. 4 Click the activation profile and click **Policy Profile**. 5 Select **Activation policy based on adapter MAC address** from the drop-down menu.

Table 5-13. Host Profile Options that Prompt for Security User Input

Information to Request User Input For	Setting the Host Profile Option
Administrator password for ESXi host when the host boots for the first time.	1 Select **Edit Host Profile**, click **Security Settings** and click **Security configuration**. 2 In the right panel, select **User Input Password to be Used to Configure Administrator Password** from the **Administrator password** drop-down menu.
Preconfigures a user for the ESXi host but prompts for the password for that user on each host when the host boots for the first time.	You can perform this task only if a user configuration already exists. Configure the user by selecting one of the options. ■ **Assigned fixed user configurations** is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear. ■ **Assign advanced fixed user configurations** is for users of ESXi 5.0 and later systems. ■ **Specify the user configuration in the profile but prompt for password during host configuration** allows you to specify the information about the user but prompt for a password on each host.
Prompt the user for credentials when the host joins the Active Directory domain.	1 Set the Authentication configuration profile to use a fixed domain. a Select **Edit Host Profile**, click **Security and Services** and click **Authentication configuration**. b Click **Active Directory configuration**. c In the Domain Name drop-down menu, select **Configure a fixed domain name**. 2 Set the method for joining the domain to prompt the user. a Select **Edit Host Profile**, click **Security and Services** and click **Authentication configuration**. b Click **Active Directory configuration**. c In the Join Domain Method drop-down menu, select **Use user specified AD credentials to join the host to domain**.

Table 5-14. Host Profile Options that Prompt for Networking User Input

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the MAC address for a port group. You can have the system prompt the user in all cases (User specified MAC address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network**. 3 In the **Determine how MAC address for vmknic should be decided** field, and select how the system manages the MAC address. ■ **User specified MAC Address to be used while applying the configuration** ■ **Prompt the user for the MAC Address if no default is available**
Prompt the user for the IPv4 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv4 address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network** and click**IP address settings**. 3 In the **IPv4 address** field, select how the system manages the IPv4 address. ■ **User specified IPv4 Address to be used while applying the configuration** ■ **Prompt the user for the IPv4 Address if no default is available**
Prompt the user for the IPv6 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv6 address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network** and click **IP address settings**. 3 In the **Static IPv6 address** field, select how the system manages the IPv4 address. ■ **User specified IPv6 Address to be used while applying the configuration** ■ **Prompt the user for the IPv6 Address if no default is available**
Prompt the user for the DNS name of the host. You can have the system prompt the user in all cases (User specified host name...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **DNS configuration**. 2 In the Host name field, select how the system manages the DNS configuration. ■ **Prompt the user for host name if default is not available** ■ **User specified host name to be used while applying the configuration**
Prompt the user for the MAC address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user in all cases or only if no default is available.	1 Open **Networking configuration**. 2 Click **Host virtual NIC**. 3 In the **Determine how MAC address for vmknic should be decided** field, select how the system manages the MAC address for the distributed switch. ■ **User specified MAC address to be used while applying the configuration** ■ **Prompt the user for the MAC address if no default is available**

Table 5-14. Host Profile Options that Prompt for Networking User Input (Continued)

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the IPv4 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Click **Host virtual NIC**. 3 Click **IP address settings**. 4 In the IPv4 address field, select how the system handles the IPv4 address for the distributed switch. ■ **User specified IPv4 address to be used while applying the configuration** ■ **Prompt the user for IPv4 address if no default is available**
Prompt the user for the IPv6 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Open **Host virtual NIC**. 3 Open **IP address settings**. 4 In the **Static IPv6 address** field, select how the system manages the IPv6 address for the distributed switch. ■ **User specified IPv6 address to be used while applying the configuration** ■ **Prompt the user for IPv6 address if no default is available**

Auto Deploy Best Practices and Security Consideration

Follow best practices when installing vSphere Auto Deploy and when using Auto Deploy with other vSphere components. Set up a highly available Auto Deploy infrastructure in large production environments or when using stateless caching. Follow all security guidelines that you would follow in a PXE boot environment, and consider the recommendations in this chapter.

Auto Deploy Best Practices

This section discusses several Auto Deploy best practices. See the VMware Knowledge Base for additional best practice information.

Auto Deploy and vSphere HA Best Practices

You can improve the availability of the virtual machines running on hosts provisioned with Auto Deploy by following best practices.

- Some environments configure the hosts provisioned with Auto Deploy with a distributed switch or configure virtual machines running on the hosts with Auto Start Manager. In those environments, deploy the vCenter Server system so that its availability matches the availability of the Auto Deploy server. Several approaches are possible.
  - In a proof of concept environment, deploy the vCenter Server system and the Auto Deploy server on the same system. In all other situations, install the two servers on separate systems.
  - Deploy vCenter Server Heartbeat.

    VMware vCenter Server Heartbeat delivers high availability for VMware vCenter Server, protecting the virtual and cloud infrastructure from application, configuration, operating system, or hardware related outages.

- Deploy the vCenter Server system in a virtual machine. Run the vCenter Server virtual machine in a vSphere HA enabled cluster and configure the virtual machine with a vSphere HA restart priority of high. Include two or more hosts in the cluster that are not managed by Auto Deploy and pin the vCenter Server virtual machine to these hosts by using a rule (vSphere HA DRS required VM to host rule). You can set up the rule and then disable DRS if you do not wish to use DRS in the cluster. The greater the number of hosts that are not managed by Auto Deploy the greater your resilience to host failures.

  NOTE This approach is not suitable if you use Auto Start Manager because Auto Start Manager is not supported in a cluster enabled for vSphere HA.

Auto Deploy Networking Best Practices

Prevent networking problems by following Auto Deploy networking best practices.

IP Address Allocation Using DHCP reservations is highly recommended for address allocation. Fixed IP addresses are supported by the host customization mechanism, but providing input for each host is cumbersome and not recommended.

VLAN Considerations Using Auto Deploy in environments that do not use VLANs is highly recommended.

If you intend to use Auto Deploy in an environment that uses VLANs, you must make sure that the hosts you want to provision can reach the DHCP server. How hosts are assigned to a VLAN depends on the setup at your site. The VLAN ID might be assigned by the switch or by the router, or you might be able to set the VLAN ID in the host's BIOS or through the host profile. Contact your network administrator to determine the steps for allowing hosts to reach the DHCP server.

Auto Deploy and VMware Tools Best Practices

See the VMware Knowledge Base article 2004018 for Auto Deploy and VMware Tools best practices.

Auto Deploy Load Management Best Practice

Simultaneously booting large numbers of hosts places a significant load on the Auto Deploy server. Because Auto Deploy is a web server at its core, you can use existing web server scaling technologies to help distribute the load. For example, one or more caching reverse proxy servers can be used with Auto Deploy. The reverse proxies serve up the static files that make up the majority of an ESXi boot image. Configure the reverse proxy to cache static content and pass all requests through to the Auto Deploy server. See the VMware Techpubs Video *Using Reverse Web Proxy Servers for Auto Deploy*.

Configure the hosts to boot off the reverse proxy by using multiple TFTP servers, one for each reverse proxy server. Finally, set up the DHCP server to send different hosts to different TFTP servers.

When you boot the hosts, the DHCP server sends them to different TFTP servers. Each TFTP server sends hosts to a different server, either the Auto Deploy server or a reverse proxy server, significantly reducing the load on the Auto Deploy server.

After a massive power outage, VMware recommends that you bring up the hosts on a per-cluster basis. If you bring up multiple clusters simultaneously, the Auto Deploy server might experience CPU bottlenecks. All hosts come up after a potential delay. The bottleneck is less severe if you set up the reverse proxy.

vSphere Auto Deploy Logging and Troubleshooting Best Practices

To resolve problems you encounter with vSphere Auto Deploy, use the Auto Deploy logging information from the vSphere Client and set up your environment to send logging information and core dumps to remote hosts.

Auto Deploy Logs (vSphere Client)

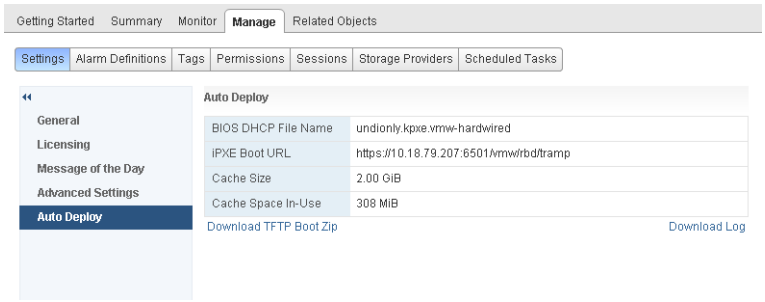
1. From a vSphere Client, connect to the vCenter Server system that Auto Deploy is associated with.
2. When the Certificate warning appears, select the check box, click **Ignore** and repeat if a second warning appears.
3. In the vSphere Client, click Home.

   An Auto Deploy icon is included in the display.
4. Click the Auto Deploy icon to display the Auto Deploy page.

5. In the Auto Deploy page, click **Download AutoDeploy Log Files**.

Auto Deploy Logs (vSphere Web Client)

1. In a vSphere Web Client connected to the vCenter Server system that Auto Deploy is registered with, go to the inventory list and select the vCenter Server system.
2. Click the Manage tab, select Settings, and click Auto Deploy.
3. Click **Download TFTP Boot Log** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.



Setting Up Syslog

Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.

Setting Up ESXi Dump Collector

Hosts provisioned with Auto Deploy do not have a local disk to store core dumps on. Install ESXi Dump Collector and set up your first host so all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts. See "Configure ESXi Dump Collector with ESXCLI," on page 99 and "Set Up ESXi Dump Collector from the Host Profiles Interface in the vSphere Client," on page 100.

Using Auto Deploy in a Production Environment

When you move from a proof of concept setup to a production environment, take care to make the environment resilient.

- Protect the Auto Deploy server. "Auto Deploy and vSphere HA Best Practices," on page 117 gives an overview of the options you have.
- Protect all other servers in your environment including the DHCP server and the TFTP server.
- Follow VMware security guidelines, including those outlined in "Auto Deploy Security Considerations," on page 121.

Set up a Highly Available Auto Deploy Infrastructure

In many production situations, a highly available Auto Deploy infrastructure is required to prevent data loss. Such an infrastructure is also a prerequisite for using Auto Deploy with stateless caching.

Prerequisites

For the management cluster, install ESXi on three hosts. Do not provision the management cluster hosts with Auto Deploy.

Procedure

1 Enable vSphere HA and vSphere DRS on the management cluster.

2 Set up the following virtual machines on the management cluster.

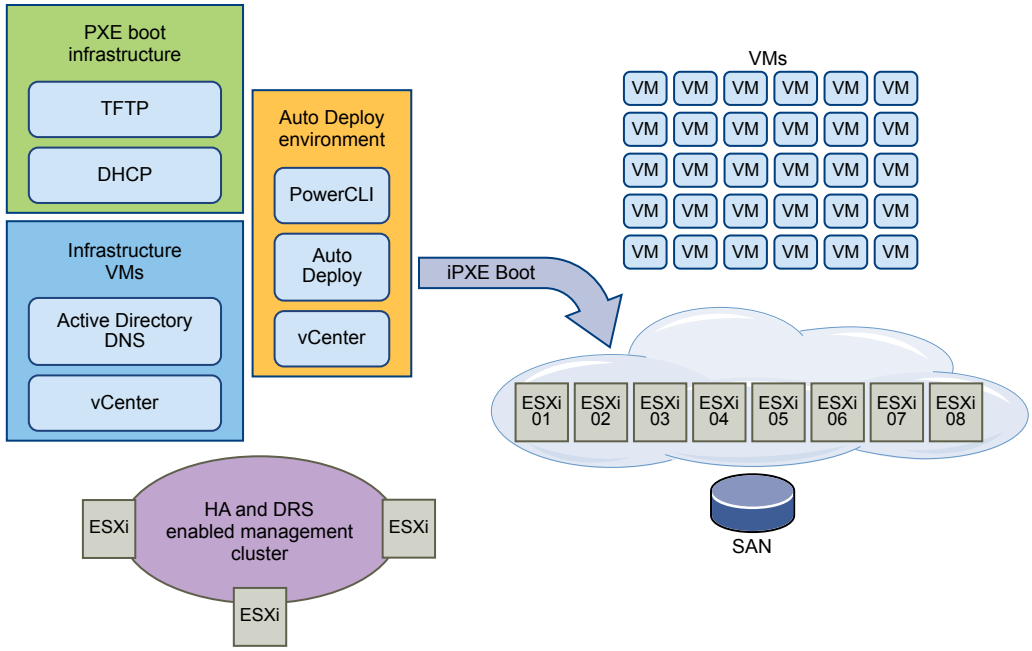
Infrastructure component	Description
PXE boot infrastructure	TFTP and DHCP servers.
Infrastructure VM	Active Directory, DNS, vCenter Server.
Auto Deploy environment	PowerCLI, Auto Deploy server, vCenter Server. Set up this environment on a single virtual machine or on three separate virtual machines in production systems.

The vCenter Server on the infrastructure virtual machine differs from the vCenter Server in the Auto Deploy environment.

3 Set up Auto Deploy to provision other hosts as needed.

Because the components on the management cluster are protected with vSphere HA, high availability is supported.

Figure 5-5. Highly Available Auto Deploy Infrastructure



Auto Deploy Security Considerations

Understanding potential security risks helps you set up your environment in a secure manner.

Secure your network as you would for any other PXE-based deployment method. Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or of the Auto Deploy server is not checked during a PXE boot.

The boot image that the Auto Deploy server downloads to a machine can have the following components.

- The VIB packages that the image profile consists of are always included in the boot image.
- The host profile and host customization are included in the boot image if Auto Deploy rules are set up to provision the host with a host profile or a host customization setting.
  - The administrator (root) password and user passwords that are included with host profile and host customization are MD5 encrypted.
  - Any other passwords associated with profiles are in the clear. If you set up Active Directory by using host profiles, the passwords are not protected.

    Use the vSphere Authentication Service for setting up Active Directory to avoid exposing the Active Directory passwords.
- The host's public and private SSL key and certificate are included in the boot image.

You can greatly reduce the security risk of Auto Deploy by completely isolating the network where Auto Deploy is used.

Troubleshooting Auto Deploy

The Auto Deploy troubleshooting topics offer solutions for situations when provisioning hosts with Auto Deploy does not work as expected.

Auto Deploy TFTP Timeout Error at Boot Time

A TFTP Timeout error message appears when a host provisioned by Auto Deploy boots. The text of the message depends on the BIOS.

Problem

A TFTP Timeout error message appears when a host provisioned by Auto Deploy boots. The text of the message depends on the BIOS.

Cause

The TFTP server is down or unreachable.

Solution

- Ensure that your TFTP service is running and reachable by the host that you are trying to boot.

Auto Deploy Host Boots with Wrong Configuration

A host is booting with a different ESXi image, host profile, or folder location than the one specified in the rules.

Problem

A host is booting with a different ESXi image profile or configuration than the image profile or configuration that the rules specify. For example, you change the rules to assign a different image profile, but the host still uses the old image profile.

Cause

After the host has been added to a vCenter Server system, the boot configuration is determined by the vCenter Server system. The vCenter Server system associates an image profile, host profile, or folder location with the host.

Solution

- Use the `Test-DeployRuleSetCompliance` and `Repair-DeployRuleSetCompliance` PowerCLI cmdlets to reevalute the rules and to associate the correct image profile, host profile, or folder location with the host.

Host Is Not Redirected to Auto Deploy Server

During boot, a host that you want to provision with Auto Deploy loads iPXE. The host is not redirected to the Auto Deploy server.

Problem

During boot, a host that you want to provision with Auto Deploy loads iPXE. The host is not redirected to the AutoDeploy server.

Cause

The `tramp` file that is included in the TFTP ZIP file has the wrong IP address for the Auto Deploy server.

Solution

- Correct the IP address of the Auto Deploy server in the `tramp` file, as explained in the *vSphere Installation and Setup* documentation.

Auto Deploy Host with a Built-In USB Flash Drive Does Not Send Coredumps to Local Disk

If your Auto Deploy host has a built-in USB flash drive, and an error results in a coredump, the coredump is lost. Set up your system to use ESXi Dump Collector to store coredumps on a networked host.

Problem

If your Auto Deploy host has a built-in USB Flash, and if it encounters an error that results in a coredump, the coredump is not sent to the local disk.

Solution

1 Install ESXi Dump Collector on a system of your choice.

   ESXi Dump Collector is included with the vCenter Server installer.

2 Use ESXCLI to configure the host to use ESXi Dump Collector.

```
esxcli conn_options system coredump network set IP-addr,port
esxcli system coredump network set –e true
```

3 Use ESXCLI to disable local coredump partitions.

```
esxcli conn_options system coredump partition set –e false
```

Package Warning Message When You Assign an Image Profile to Auto Deploy Host

When you run a PowerCLI cmdlet that assigns an image profile that is not Auto Deploy ready, a warning message appears.

Problem

When you write or modify rules to assign an image profile to one or more hosts, the following error results:

```
Warning: Image Profile <name-here> contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.
```

Cause

Each VIB in an image profile has a `stateless-ready` flag that indicates that the VIB is meant for use with Auto Deploy. You get the error if you attempt to write an Auto Deploy rule that uses an image profile in which one or more VIBs have that flag set to FALSE.

NOTE You can use hosts provisioned with Auto Deploy that include VIBs that are not stateless ready without problems. However booting with an image profile that includes VIBs that are not stateless ready is treated like a fresh install. Each time you boot the host, you lose any configuration data that would otherwise be available across reboots for hosts provisioned with Auto Deploy.

Solution

1 Use Image Builder PowerCLI cmdlets to view the VIBs in the image profile.

2 Remove any VIBs that are not stateless-ready.

3 Rerun the Auto Deploy PowerCLI cmdlet.

Auto Deploy Host Reboots After Five Minutes

An Auto Deploy host boots and displays iPXE information, but reboots after five minutes.

Problem

A host to be provisioned with Auto Deploy boots from iPXE and displays iPXE information on the console. However, after five minutes, the host displays the following message to the console and reboots.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

The host might also display the following details:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

The console then displays the host's machine attributes including vendor, serial number, IP address, and so on.

Cause

No image profile is currently associated with this host.

Solution

You can temporarily assign an image profile to the host by running the `Apply-EsxImageProfile` cmdlet.

You can permanently assign an image profile to the host as follows.

1. Run the `New-DeployRule` cmdlet to create a rule that includes a pattern that matches the host with an image profile.
2. Run the `Add-DeployRule` cmdlet to add the rule to a ruleset.
3. Run the `Test-DeployRuleSetCompliance` cmdlet and use the output of that cmdlet as the input to the `Repair-DeployRuleSetCompliance` cmdlet.

Auto Deploy Host Does Not Network Boot

The host you provision with Auto Deploy comes up but does not network boot.

Problem

When you attempt to boot a host provisioned with Auto Deploy, the host does not start the network boot process.

Cause

You did not enable your host for network boot.

Solution

1 Reboot the host and follow the on-screen instructions to access the BIOS configuration.

If you have an EFI host, you must switch the EFI system to BIOS compatibility mode.

2 In the BIOS configuration, enable Network Boot in the Boot Device configuration.

Auto Deploy Host Does Not Get a DHCP Assigned Address

The host you provision with Auto Deploy fails to get a DHCP Address.

Problem

When you attempt to boot a host provisioned with Auto Deploy, the host performs a network boot but is not assigned a DHCP address. The Auto Deploy server cannot provision the host with the image profile.

Cause

You might have a problem with the DHCP service or with the firewall setup.

Solution

1 Check that the DHCP server service is running on the Windows system on which the DHCP server is set up to provision hosts.

a Click **Start > Settings > Control Panel > Administrative Tools**.

b Double-click **Services** to open the Services Management panel.

c In the Services field, look for the DHCP server service and restart the service if it is not running.

2 If the DHCP server is running, recheck the DHCP scope and the DHCP reservations that you configured for your target hosts.

If the DHCP scope and reservations are configured correctly, the problem most likely involves the firewall.

3 As a temporary workaround, turn off the firewall to see whether that resolves the problem.

a Open the command prompt by clicking **Start > Program > Accessories > Command prompt**.

b Type the following command to temporarily turn off the firewall. Do not turn off the firewall in a production environment.

```
netsh firewall set opmode disable
```

c Attempt to provision the host with Auto Deploy.

d Type the following command to turn the firewall back on.

```
netsh firewall set opmode enable
```

4 Set up rules to allow DHCP network traffic to the target hosts.

See the firewall documentation for DHCP and for the Windows system on which the DHCP server is running for details.

Auto Deploy Host Cannot Contact TFTP Server

The host that you provision with Auto Deploy cannot contact the TFTP server.

Problem

When you attempt to boot a host provisioned with Auto Deploy, the host performs a network boot and is assigned a DHCP address by the DHCP server, but the host cannot contact the TFTP server.

Cause

The TFTP server might have stopped running, or a firewall might block the TFTP port.

Solution

- If you installed the WinAgents TFTP server, open the WinAgents TFTP management console and verify that the service is running. If the service is running, check the Windows firewall's inbound rules to make sure the TFTP port is not blocked. Turn off the firewall temporarily to see whether the firewall is the problem.
- For all other TFTP servers, see the server documentation for debugging procedures.

Auto Deploy Host Cannot Retrieve ESXi Image from Auto Deploy Server

The host that you provision with Auto Deploy stops at the iPXE boot screen.

Problem

When you attempt to boot a host provisioned with Auto Deploy, the boot process stops at the iPXE boot screen and the status message indicates that the host is attempting to get the ESXi image from the Auto Deploy server.

Cause

The Auto Deploy service might be stopped or the Auto Deploy server might be unaccessible.

Solution

1 Log in to the system on which you installed the Auto Deploy server.

2 Check that the Auto Deploy server is running.

   a Click **Start > Settings > Control Panel > Administrative Tools**.

   b Double-click **Services** to open the Services Management panel.

   c In the Services field, look for the VMware vSphere Auto Deploy Waiter service and restart the service if it is not running.

3 Open a Web browser, enter the following URL, and check whether the Auto Deploy server is accessible.

   https://*Auto_Deploy_Server_IP_Address*:*Auto_Deploy_Server_Port*/vmw/rdb

   NOTE Use this address only to check whether the server is accessible.

4 If the server is not accessible, a firewall problem is likely.

   a Try setting up permissive TCP Inbound rules for the Auto Deploy server port.

   The port is 6501 unless you specified a different port during installation.

   b As a last resort, disable the firewall temporarily and enable it again after you verified whether it blocked the traffic. Do not disable the firewall on production environments.

   To disable the firewall, run **`netsh firewall set opmode disable`**. To enable the firewall, run **`netsh firewall set opmode enable`**.

Recovering from Database Corruption on the Auto Deploy Server

In some situations, you might have a problem with the Auto Deploy database. The most efficient recovery option is to replace the existing database file with the most recent backup.

Problem

When you use Auto Deploy to provision the ESXi hosts in your environment, you might encounter a problem with the Auto Deploy database.

IMPORTANT This is a rare problem. Follow all other Auto Deploy troubleshooting strategies before you replace the current database file. Rules or associations that you created since the backup you choose are lost.

Cause

This problem happens only with hosts that are provisioned with Auto Deploy.

Solution

1 Stop the Auto Deploy server service.

2 Find the Auto Deploy log by going to the Auto Deploy page in the vSphere Client or the vSphere Web Client.

3 Check the logs for the following message:

```
DatabaseError: database disk image is malformed.
```

If you see the message, replace the existing database with the most recent backup.

4 Go to the Auto Deploy data directory.

Operating System	File Location
vCenter Server appliance	`/var/lib/rbd`
Microsoft Windows	The data directory you selected during installation. To find it, type the following command into a command prompt. `reg.exe QUERY "HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware vSphere Auto Deploy" /v DataPath`

The directory contains a file named `db`, and backup files named `db-`*`yyy-mm-dd`*.

5 Rename the current `db` file.

VMware Support might ask for that file if you call for assistance.

6 Rename the most recent backup to `db`.

7 Restart the Auto Deploy server service.

8 If the message still appears in the log, repeat the steps to use the next recent backup until Auto Deploy works without database errors.

Problems if You Upgrade vCenter Server But Do Not Upgrade Auto Deploy Server

When you upgrade vCenter Server to vSphere 5.1, you can upgrade the Auto Deploy Server at the same time. If you postpone the update, problems with the vSphere HA agent might result.

Problem

When you upgrade vCenter Server, vCenter Server replaces the vSphere HA agent (vmware-fdm) version 5.0 with vSphere HA agent version 5.1 on each ESXi host. On hosts provisioned with Auto Deploy, the replacement is not permanent because no state is on the host. If vCenter Server is not available, the ESXi hosts do not have the correct vSphere HA agent and cannot join a cluster.

Cause

The Auto Deploy 5.0 server does not automatically upgrade the FDM VIB to version 5.1. Unless you create a new image that includes the VIB, Auto Deploy reverts to the FDM VIB version 5.0 after reboot.

Solution

Upgrade the Auto Deploy server.

If you cannot upgrade the Auto Deploy server, you can use Image Builder PowerCLI cmdlets included with vSphere PowerCLI to create an ESXi 5.0 image profile that includes the new vmware-fdm VIB. You can supply your hosts with that image profile.

1 At the PowerCLI prompt, add the ESXi 5.0 software depot and add the software depot that contains the new vmware-fdm VIB.

```
Add-EsxSoftwareDepot
C:\Path\VMware-Esxi-5.0.0-buildnumber-depot.zip

Add-EsxSoftwareDepot http://vcenter_server/vSphere-HA-depot
```

2 Create a rule that assigns the new image profile to your hosts, and add the rule to the ruleset.

```
New-DeployRule -Name "Rule Name"
-Item "ImageName"
-Pattern "my host pattern"
Add-DeployRule -DeployRule "Rule Name"
```

3 Perform a test-and-repair compliance operation for the hosts to permanently include the vSphere HA agent on the hosts.

```
$result = Test-DeployRuleSetCompliance Host_list
Repair-DeployRuleSetCompliance -TestResult $result
```

Auto Deploy Proof of Concept Setup

A proof of concept setup of an Auto Deploy environment helps administrators to evaluate the product and demonstrate its capabilities to management. When you complete the proof of concept setup workflow, you have a working Auto Deploy environment that includes a reference host and one or more other target hosts.

The proof of concept setup is intended for a test or development environment, but your completed setup can be the basis for a production environment. The set of tasks starts in an environment in which no Auto Deploy components are installed. The task descriptions assume that you are using a flat network with no VLAN tagging between the physical hosts and the rest of your environment.

To perform the tasks, you should have the following background knowledge and privileges.

- Experience with vSphere (vCenter Server, ESX, and ESXi).
- Basic knowledge of Microsoft PowerShell and vSphere PowerCLI.

- Administrator rights to the target Windows and vCenter Server systems.

Follow the tasks in the order presented in this document. Some steps can be performed in a different order, but the order used here limits repeated manipulation of some components.

You can set up a mixed-mode environment that includes an IPv6 vCenter Server. The Auto Deploy server must have an IPv4 address because PXE booting is supported only with IPv4.

Proof of Concept Preinstallation Checklist

Before you can start the proof of concept setup, make sure that your environment meets the hardware and software requirements and that you have the necessary permissions for the components that are included in the setup.

You need the following hardware and software for your proof of concept setup.

- vCenter Server 5.1 installed on a Windows system. In this proof of concept setup, you install the Auto Deploy server and the vSphere PowerCLI on the host on which the vCenter Server is running. You perform many of the setup tasks by logging in to that host, either directly into the console or by using Remote Desktop (RDP).
  - Datacenter, clusters, and folders configured on the vCenter Server system.
  - At least 4GB of free space on the vCenter Server system. Preferably a second volume or hard drive.
- Storage for ESXi datastores (NFS, iSCSI, or FibreChannel), with servers and storage arrays that are configured so the servers can see the LUNs.
  - List of target IP addresses for NFS or iSCSi.
  - List of target volume information for NFS or iSCSI.
- Two or more hosts to be provisioned with Auto Deploy, and the following information for each host.
  - List of MAC addresses for each physical NIC.
  - List of IP addresses and fully qualified host names preassigned for target ESXi installs.
    - Default route, netmask, and primary and secondary DNS server IP addresses.
    - IP address and netmask for the VMkernel primary (management) network.
    - IP address and netmask for other VMkernel networks such as storage, vSphere FT, or VMware vMotion.

  Auto Deploy does not overwrite existing partitions by default.
- vSphere installer (DVD or ISO).
- Window 7 or Windows Server 2008 system with Microsoft PowerShell preinstalled.
- vSphere PowerCLI installer binaries downloaded from the Downloads page on the VMware Web site.
- Location of the ESXi software depot on the Downloads page of the VMware Web site. You will use a URL to point to the image profile stored at that location or download a ZIP file to work with a local depot. Do not download the ESXi 5.1 image.
- TFTP installer software such as WinAgents TFTP server. The TFTP server included in Windows 2008 is closely tied to Windows network deployment and is not suitable.
- DHCP server. The DHCP server included with Windows 2008 is suitable for this proof of concept setup.

You also need information about and administrator privileges to the environment's core servers including the ActiveDirectory server, DNS server, DHCP server, NTP server, and so on.

You must have complete control of the broadcast domain of the subnet in which you will deploy the setup. Ensure that no other DHCP, DNS, or TFTP server are on this subnet.

Install the TFTP Server

Auto Deploy relies on a TFTP server for sending the boot image to the hosts that it provisions. You must install a TFTP server in your environment.

This task only installs the TFTP server. You later download a configuration file to the server. See "Configure the Auto Deploy and TFTP Environment in the vSphere Client," on page 135.

Prerequisites

Make sure your system meets the requirements in the Preinstallation Checklist. See "Proof of Concept Preinstallation Checklist," on page 129.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

2 Download and install the TFTP server software.

This sample setup uses the TFTP server from WinAgents. The TFTP server that is included with Windows 2008 is closely tied to Windows network deployment and not suitable for Auto Deploy.

3 Configure the TFTP root directory as D:*Drive* or a similar location (for example, `D:\TFTP_Root\`).

What to do next

Install and set up vSphere PowerCLI. You use PowerCLI cmdlets to write the rules that assign image profiles and host profiles to hosts. See "Install and Set Up vSphere PowerCLI," on page 130.

Install and Set Up vSphere PowerCLI

You manage Auto Deploy with rules that you create with vSphere PowerCLI cmdlets.

This proof of concept setup installs vSphere PowerCLI on the same system as the vCenter Server system. You can also install PowerCLI on a different Windows system.

Prerequisites

- Verify that Microsoft .NET 2.0 is installed, or install it from the Microsoft Web site following the instructions on that Web site.
- Verify that Microsoft Powershell 2.0 is installed, or install it from the Microsoft website following the instructions on that Web site.

PowerShell 2.0 is preinstalled on Windows 2008 and Windows 7 systems.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly by using RDP.

2 Open a command prompt and type the following commands in sequence, pressing Enter after each line.

```
powershell
Set-ExecutionPolicy RemoteSigned
Exit
```

3 Download vSphere PowerCLI from the Download page of the VMware Web site and install the vSphere PowerCLI software.

4 Confirm that PowerCLI is working.

   a Double-click the PowerCLI icon on the desktop to open a PowerCLI window.

   b Ignore the SSL error, type **`Get-DeployCommand`**, and press Enter.

   PowerCLI displays a list of cmdlets and their definitions in the PowerCLI window.

What to do next

- If you do not see a list of cmdlets when you run `Get-DeployCommand`, check your PowerCLI version and uninstall and reinstall if necessary.
- For some background information on PowerCLI, see "Using Auto Deploy Cmdlets," on page 79. See the vSphere PowerCLI documentation set for details.
- Prepare the hosts you want to provision with Auto Deploy. See "Prepare Auto Deploy Target Hosts," on page 131.

Prepare Auto Deploy Target Hosts

You must prepare all target hosts for Auto Deploy.

Prerequisites

Hosts that you want to provision with Auto Deploy must meet the requirements for ESXi.

See "ESXi Hardware Requirements," on page 29.

NOTE You cannot provision EFI hosts with Auto Deploy unless you switch the EFI system to BIOS compatibility mode.

Procedure

1 Change each physical host's BIOS settings to force the host to boot from the primary network device.

2 Reconfirm the MAC address of the primary network device.

What to do next

Prepare the DHCP Server. See "Prepare the DHCP Server," on page 131.

Prepare the DHCP Server

The DHCP Server in your proof of concept environment must be set up to serve each target host with an iPXE binary.

The proof of concept environment uses Active Directory with DNS and DHCP.

The proof of concept illustrates how to use DHCP reservations. Setting up fixed IP addresses for each host is time consuming and not recommended.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Log in to your DHCP Server as an administrator user.

2 Create a DHCP scope for your IP address range.

   a Click **Start > Settings > Control Panel > Administrative Tools** and click **DHCP**.

   b Drill down to **DHCP >** ***hostname*** **> IPv4**, right click, and click **New Scope**.

   c Click **Next** on the Welcome screen and specify a name and description for the scope.

   d Specify an IP address range and click **Next**.

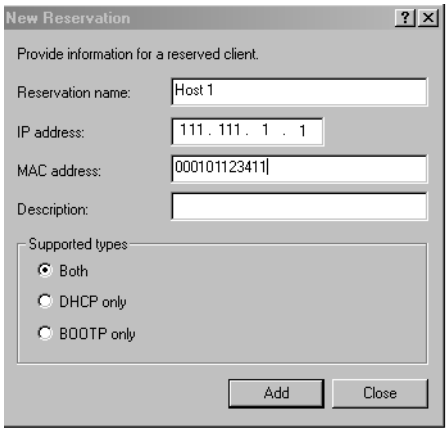
   e Click **Next** until you reach the Configure DHCP Options screen and select **No, I will configure this option later**.

3 If you are planning on using DHCP reservations, create a DHCP reservation for each target ESXi host.

   a In the DHCP window, drill down to **DHCP >** ***hostname*** **> IPv4 > Autodeploy Scope > Reservations**.

   b Right-click **Reservations** and select **New Reservation**.

   c In the New Reservation window, specify a name, IP address, and the MAC address for one of the hosts. Do not include the colon (:) in the MAC address.



   d Repeat the process for each of the other hosts.

4 Set up the DHCP Server to point the hosts to the TFTP Server.

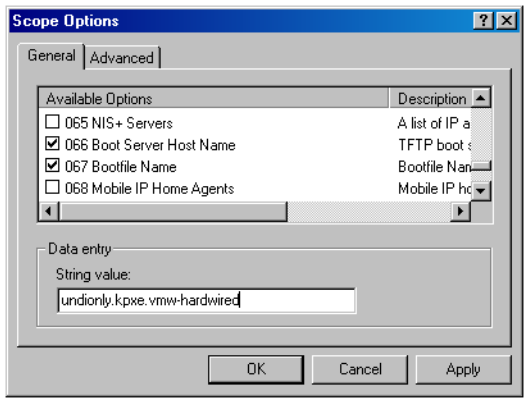
   The precise process depends on the DHCP Server you are using. This example uses the DHCP server included with Windows 2008.

   a In the DHCP window, drill down to **DHCP >** ***hostname*** **> IPv4 > Autodeploy Scope > Scope Options**.

   b Right click **Scope Options** and choose **Configure Options**.

   c In the Scope Options window, click the **General** tab.

d Click **066 Boot Server Host Name** and enter the address of the TFTP server that you installed in the String value field below the Available Options.



e Click **067 Bootfile Name** and enter **`undionly.kpxe.vmw-hardwired`**.

The `undionly.kpxe.vmw-hardwired` iPXE binary will be used to boot the ESXi hosts.

f Click **Apply** and click **OK** to close the window.

5 In the DHCP window, right-click **DHCP > *hostname* > IPv4 > Scope > Activate** and click **Activate**.

6 Do not log out from the DHCP Server if you are using Active Directory for DHCP and DNS, or log out otherwise.

What to do next

Prepare the DNS Server. See "Prepare the DNS Server," on page 133.

Prepare the DNS Server

Preparing the DNS server involves adding the DHCP information to the DNS server and verifying that the DNS entries are working. This task is optional.

The example environment uses Active Directory with DNS and DHCP.

Prerequisites

Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Log in to the DNS server.

2 Add the DHCP reservation IP addresses and the associated host names as static DNS entries.

Be sure to add entries in both Forward (ARecord) and Reverse (PTR Record) Zones.

3 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

4 Open a command prompt and perform an nslookup of ESXi host names to validate that the DNS entries are working.

Use both forward (Short and FQDN) and reverse lookups.

5 Log out of your DNS server.

What to do next

Install the Auto Deploy Server software. See "Install Auto Deploy Server Software," on page 134.

Install Auto Deploy Server Software

Auto Deploy server software is included with the vCenter Server installation media. This proof of concept setup installs the Auto Deploy server on the system on which vCenter Server is installed.

If you are using vCenter Server 5.1, install Auto Deploy server 5.1. If you have an Auto Deploy 5.0 server installed and you cannot upgrade the Auto Deploy server, see "Problems if You Upgrade vCenter Server But Do Not Upgrade Auto Deploy Server," on page 128.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

2 Secure the installation media for the Auto Deploy server software.

vCenter Server type	Action
Virtual	Download the vSphere installer CD ISO image and place the ISO on a data store the vCenter Server can access.
Physical	Download the vSphere installer CD ISO image and burn it to disk.

3 Make the ISO available to the vCenter Server.

vCenter Server type	Action
Virtual	Attach the CD-ROM drive to the ISO, either by using the vSphere Client or from the datastore.
Physical	Insert the DVD into the physical server's drive.

4 Run Autoplay on the DVD.

5 Select Auto Deploy Server and click **Install**.

6 When the installer wizard prompts you for the Repository Location, browse to the volume or hard drive that has enough storage for Auto Deploy use and select that location.

Network shares are not an option when you install Auto Deploy.

7 Leave the defaults for everything else.

8 When the installer prompts you for credentials, use your vCenter Server administrator credentials.

What to do next

- Verify that you have access to a one of the vSphere client interfaces.
  - Request access to a vSphere Web client that can access the vCenter Server system that will manage the Auto Deploy server.
  - Install the vSphere Client if you intend to use that client interface.

- Configure the Auto Deploy and TFTP environment. See "Configure the Auto Deploy and TFTP Environment in the vSphere Client," on page 135.

Configure the Auto Deploy and TFTP Environment

You can configure the Auto Deploy and TFTP Environment in the vSphere Client or in the vSphere Web Client.

Configure the Auto Deploy and TFTP Environment in the vSphere Client

You must download a TFTP Boot ZIP file from your Auto Deploy server. The customized TFTP server serves the boot images that Auto Deploy provides. You can perform the task in the vSphere Client.

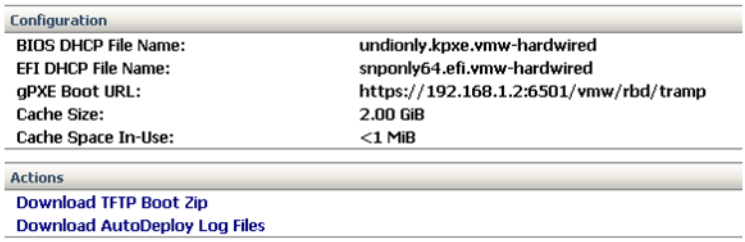
Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1. From a vSphere Client, connect to the vCenter Server system, which is localhost in this proof of concept setup.
2. When the Certificate warning appears, select the check box, click **Ignore**, and repeat this process if a second warning appears.
3. In the vSphere Client, click **Home**.

   An Auto Deploy icon is included in the display.
4. (Optional) If the Auto Deploy icon is missing, select **Plugins > Manage Plugins**, ensure Auto Deploy is enabled, and close the Plugins dialog.
5. Click the Auto Deploy icon to display the Auto Deploy page.
6. In the Auto Deploy page, click **Download TFTP Boot ZIP** in the Actions box.



7. Save the file (`Deploy-tftp.zip`) to the TFTP_Root directory that you created when you installed the TFTP Server and unzip the file into that directory.
8. Close the file browser and minimize the vSphere Client.

What to do next

Prepare the depot from which Auto Deploy retrieves the ESXi software when it provisions the hosts. See "Prepare the ESXi Software Depot," on page 136.

Configure the Auto Deploy and TFTP Environment in the vSphere Web Client

You must download a FTP Boot ZIP file from your Auto Deploy server. The customized FTP server serves the boot images that Auto Deploy provides. You can perform the task in the vSphere Web Client.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

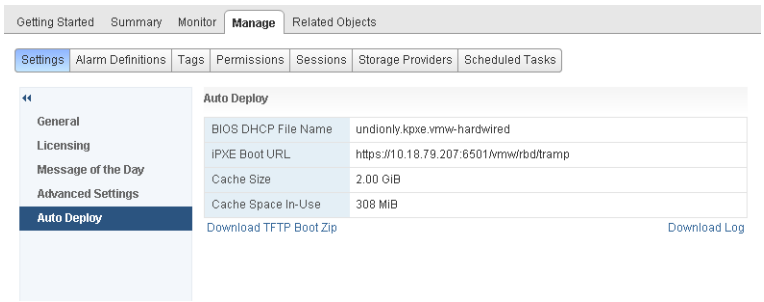
1 From your Web browser, access the URL of the vSphere Web Client that connects to the vCenter Server system which manages the Auto Deploy Server.

2 When the Certificate warning appears continue to the vCenter Server system.

3 In the inventory, drill down to the vCenter Server system.

4 Click the Manage tab, select Settings, and click Auto Deploy.

5 Click **Download TFTP Boot Log** to download the TFTP configuration file.



6 Save the file (`Deploy-tftp.zip`) to the TFTP_Root directory that you created when you installed the TFTP Server and unzip the file into that directory.

7 Minimize the Web browser you are using with the vSphere Web Client.

What to do next

Prepare the depot from which Auto Deploy retrieves the ESXi software when it provisions the hosts. See "Prepare the ESXi Software Depot," on page 136.

Prepare the ESXi Software Depot

Auto Deploy provisions hosts with images described by image profiles. Image profiles are stored in software depots. You must make sure the correct image profile is available before you start provisioning hosts.

The ESXi software depot contains the image profiles and software packages (VIBs) that are used to run ESXi. An image profile is a list of VIBs. This proof of concept setup uses a depot and image profile provided by VMware and does not create custom image profiles.

This proof of concept setup downloads the ZIP file that contains the image profile. You can instead point the Auto Deploy server to the HTTP URL of an image profile.

If you require custom VIBs such as custom drivers in your image profile, you can create a custom image profile by using the Image Builder PowerCLI.

The steps in this task instruct you to run PowerCLI cmdlets. For additional information on each cmdlet, type `Help` *cmdlet* at the PowerCLI prompt or search the vSphere Documentation Center.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1. Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.
2. Download the ESXi Depot ZIP file from the VMware Web site to a location the PowerCLI Windows system can access.

   The file has a name that follows this pattern: `VMware-Esxi-5.1.0-xxxxx-depot.zip`.
3. Save the ZIP file to your local D:\ drive or any volume with enough space and note the location of the file.
4. Start a PowerCLI session and run the following cmdlets at the prompt.

   ```
   Connect-VIServer -Server your_vc_hostname -User username -Password password <Enter>
   Add-EsxSoftwareDepot path:\VMware-Esxi-5.1.0-xxxxx-depot.zip <Enter>
   ```

   Include the complete path and file name of the ZIP file you downloaded.
5. Validate that you successfully added the ZIP file to the depot by checking the contents of the depot with the `Get-EsxImageProfile` cmdlet.

   ```
   Get-EsxImageProfile <Enter>
   ```

   The cmdlet returns information about all image profiles in the depot.

What to do next

Set up Auto Deploy to provision the first host and provision that host with the image profile in the depot. See "Set Up the First Host and Provision with Auto Deploy," on page 137.

Set Up the First Host and Provision with Auto Deploy

Setting up the first host requires that you understand how to write Auto Deploy rules with vSphere PowerCLI. After you write the rules and add them to the ruleset, you can turn on the host to provision it.

You use the PowerCLI command-line interface to specify how Auto Deploy provisions the target hosts. You define rules and add each rule to the active ruleset. The Auto Deploy server checks the ruleset to determine which image profile to send to each ESXi host, which host profile to send to each ESXi host, and which location on the vCenter Server to place the host in.

A rule allows you to specify the following parameters.

Parameter	Description	
Name	Name of the rule, specified with the `-Name` parameter.	
Item	One or more items, specified with the `-Item` parameter. An item can be an image profile to be used, a host profile to be used, or a vCenter Server inventory location (datacenter, folder, cluster) for the target host. You can specify multiple items separated by commas.	
Pattern	The pattern specifies the host or group of hosts to which the rule applies. Choose one of the following.	
	vendor	Machine vendor name.
	model	Machine model name.
	serial	Machine serial number.
	hostname	Machine hostname.
	domain	Domain name.
	ipv4	IPv4 address of the machine.
	mac	Boot NIC MAC address.
	asset	Machine asset tag.
	oemstring	OEM-specific strings in the SMBIOS.
	Specify `-AllHosts` to apply the item or items to all hosts.	

This proof of concept setup first uses `-AllHosts` and later uses an IP address range to identify the hosts to provision.

Write Rules for the First Host

You specify the image profile to provision the host with by using PowerCLI to write a rule and adding the rule to the active ruleset.

This task assumes you have a basic knowledge of Microsoft PowerShell and vSphere PowerCLI.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.
- Make sure you can access the ESXi software from the system on which you run the PowerCLI cmdlets.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

This task assumes that you installed PowerCLI on the system on which the vCenter Server system is running.

2 Open the PowerCLI window and list the ESXi image profiles.

```
Get-EsxImageProfile
```

3 Create a new rule by running the following cmdlet, replacing ESXi-5.1.0-*XXXXX*-standard with the image profile that you want to use.

```
New-DeployRule -Name "InitialBootRule" -Item "Esxi-5.1.0-XXXXX-standard" -AllHosts
```

4 Add the new rule to the active rule set to make the rule available to the Auto Deploy server.

```
Add-DeployRule -DeployRule "InitialBootRule"
```

What to do next

Boot the host and check that Auto Deploy provisions the host and adds it to the vCenter Server inventory. See "Provision the First Host," on page 139.

Provision the First Host

You can provision the first host and check its location on the vCenter Server to complete verification of the image provisioning of your setup.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1. Open a console session to the physical host that you want to use as the first ESXi target host, boot the host, and look for messages that indicate a successful iPXE boot.

   During the boot process, DHCP assigns an IP address to the host. The IP address matches a name you specified earlier in the DNS server. The host contacts the Auto Deploy server and downloads the ESXi binaries from the HTTP URL indicated in the iPXE tramp file that you downloaded into the TFTP_Root directory earlier. Each instance of Auto Deploy produces a custom set of files for the TFTP Server.

2. Open the vSphere Client or connect to the vSphere Web Client and connect to the vCenter Server system.

   In this proof of concept setup, the vCenter Server system is localhost.

3. Click **Hosts and Clusters**.

4. Check that the newly provisioned host is now in the vCenter Server inventory at the datacenter level.

   By default, Auto Deploy adds hosts at the datacenter level when the boot process completes.

What to do next

If you encounter problems, see "Troubleshooting Auto Deploy," on page 122.

Configure the first host for use as a reference host and save its host profile for use with other hosts. See "Configure the Proof of Concept Reference Host," on page 139.

Configure the Proof of Concept Reference Host

You can customize the first ESXi host that you boot for your environment and create a host profile. You can set up Auto Deploy to provision other target hosts with that host profile. The ESXi host you create the host profile from is considered your reference host or template host.

How you configure the reference host depends on what you want to do.

Shared settings	Specify settings that all hosts share and save a host profile for the host.
Host-specific settings	Customize hosts by setting up the host profile to prompt for user input for a limited number of options such as a static IP address. Host customizations are saved when you save the host profile. See "Host Customization in the vSphere Web Client," on page 113.

Auto Deploy applies all common settings from the host profile to all target hosts. If you set up the host profile to ask for user input, all hosts provisioned with that host profile come up in maintenance mode. You must reapply the host profile or reset host customizations to be prompted for the host-specific information.

NOTE Administrators cannot directly access or manipulate host customizations. Use the vSphere Client or the vSphere Web Client Host Profiles UI to work with host customizations.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to the vCenter Server system.

   In this proof of concept setup, the vCenter Server system is localhost.

2 Click Hosts and Clusters and select the host that Auto Deploy added to the first datacenter.

3 Configure the host.

   The rest of the proof of concept setup assumes that you configure at least one setting that is different for different hosts.

Configuration	Description
Networking	Configure the following networking components. ■ Base virtual switch and management port group for VMkernel. ■ Storage network port group for VMkernel. ■ Virtual machine networking port group. ■ Any additional virtual switches and port groups. ■ Distributed switches, if necessary (transfer port groups to distributed switches if you use them).
Storage	Configure shared storage.
Time settings	Configure your time settings.
Security	Configure the security profile.
Authentication	Configure authentication.
DNS and routing	If necessary, configure DNS and route settings.
Other	Configure advanced settings or any other settings as required in the target environment.

What to do next

Create the host profile from the reference host for use with all other target hosts. See the *Host Profiles* documentation.

Create a Host Profile with the vSphere Client

Configuration that is shared by a group of hosts is stored in a host profile. You can create the host profile from your reference host. Configuration that differs for different hosts, such as a static IP address, can be managed through the answer file mechanism.

Auto Deploy provisions each host with a common host profile. In certain cases, Auto Deploy also uses a host-specific answer file that allows you to specify information that differs for different hosts. For example, if you set up a VMkernel port for vMotion or for storage, you can specify a static IP address for the port by using the answer file mechanism.

In this example, you create a host profile from the reference host, attach that host profile to the same host, and create an answer file for the reference host.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 With the vSphere Client, log in to the vCenter Server system with administrator privileges.

2 Click **Home** and select **Host Profiles**.

3 Click **Create a Host Profile** in the Getting Started tab on the right.

4 In the wizard, make the following selections.

Option	Description
Creation Method	Create Profile from existing host.
Specify Reference Host	Select the host you just configured.
Profile Details	Name the profile ESXiGold and add a description.
Ready to Complete	Review the information and click **Finish**.

5 Right-click the ESXiGold host profile, select **Attach Host/Cluster**, select the ESXi host from which you created the profile, and click **OK**.

If any information is marked as user input in the host profile, you are prompted. In this example, no host profile items are set up to prompt you.

6 Put the host into maintenance mode and apply the host profile.

a Go to the Hosts and Clusters view, right-click the ESXi host, and put the host into maintenance mode.

b With the host in maintenance mode, right-click again, and select **Apply Profile**.

vCenter Server checks the host for compliance and returns Compliant after the rescan is complete.

What to do next

Create a rule that assigns the image profile and the newly-created host profile to all hosts you want to provision with Auto Deploy. See "Create a Rule for Other Target Hosts," on page 142.

Create and Apply a Host Profile with the vSphere Web Client

Configuration that is shared by a group of hosts is stored in a host profile. You can create the host profile from your reference host. Configuration that differs for different hosts, such as a static IP address, can be managed through the ahost customization mechanism.

Auto Deploy can provision each host with the same host profile. In certain cases, Auto Deploy also uses host customizations that allow you to specify information that differs for different hosts. For example, if you set up a VMkernel port for vMotion or for storage, you can specify a static IP address for the port by using the host customization mechanism.

In this example, you extract a host profile from a reference host, attach the host profile to one other host, and check host profile compliance. In most cases, you do not perform these tasks manually but you write an Auto Deploy rule that applies a host profile to hosts that are provisioned with Auto Deploy. See "Assign a Host Profile to Hosts," on page 83.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Log in to a vSphere Web Client that is connected to the vCenter Server system with administrator privileges.

2 Click **Rules and Profiles** and select **Host Profiles**.

3 Click the Extract profile from host icon and respond to the wizard prompts.

Option	Description
Select Host	Select the reference host you configured earlier.
Name and Description	Name the profile ESXiGold and add a description.
Ready to Complete	Review the information and click **Finish**.

4 Right-click the ESXiGold host profile, select **Attach/Detach Hosts and Clusters**.

5 Select the ESXi host to which you want to attach the profile, click **Attach**, and click **Next**.

The wizard loads the host customization.

6 Provide any customization information and click **Finish**.

What to do next

Create a rule that assigns the image profile and the newly-created host profile to all hosts you want to provision with Auto Deploy. See "Create a Rule for Other Target Hosts," on page 142.

Create a Rule for Other Target Hosts

You can create a rule that applies the previously verified image profile and the host profile that you just created to all target hosts.

This task assumes you have a basic knowledge of Microsoft PowerShell and vSphere PowerCLI.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

2 Start a PowerCLI session and type the following commands, followed by Enter, at the prompt.

```
Connect-VIServer -Server your_vc_hostname -User username -Password password
Add-EsxSoftwareDepot path:\VMware-Esxi-5.1.0-xxxxx-depot.zip
```

Include the complete path and file name of the ZIP file you downloaded earlier. Adding the software depot is required each time you start a new PowerCLI session.

3 (Optional) To display the rules in the active ruleset type he following cmdlet at the prompt and press Enter.

```
Get-DeployRuleset
```

4 To create a rule that instructs Auto Deploy to provision the set of hosts in the specified IP range with the image you selected and with the host profile you created from the reference host, type the following command and press Enter.

```
New-DeployRule -name "Production01Rule" -item "image_profile", ESXiGold,target_cluster -
Pattern "ipv4=IP_range"
```

Option	Description
image_profile	The ESXi image profile you used in the first deploy rule.
target_cluster	Name of the cluster in vCenter Server to which you want to add all hosts.
IP_range	Either a single IP address or a range of IP addresses for the hosts you want to provision with the image profile and host profile.

When you specify a target cluster, the host profile is applied to all hosts in the cluster. Applying the host profile to each host is not required.

5 Add the new rule to the active ruleset.

```
Add-DeployRule -DeployRule "Production01Rule"
```
<Enter>

6 (Optional) Remove the deploy rule you created for the initial boot operation.

```
Remove-DeployRule -DeployRule InitialBootRule
```
<Enter>

7 Check the active rule set.

```
Get-DeployRuleset
```
<Enter>

PowerCLI displays information similar to the following example.

```
Name:              Production01Rule
PatternList:       {ipv4=address_range}
ItemList:          {ESXi-5.1.0-XXXXXX-standard, Compute01, ESXiGold}
```

What to do next

Provision all hosts and set up host customizations for each host. See "Provision All Hosts and Set Up Host Customizations," on page 143.

Provision All Hosts and Set Up Host Customizations

With the rule in place that provisions hosts using an image profile, and with the host profile created from the reference host available, you can provision all target hosts. If any host profile items are set to prompt the user for input, the host comes up in maintenance mode. You apply the host profile or check host compliance to be prompted for the information. The system associates the host customization with the host.

Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 129.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 128 for the complete list.
- Open a console to each host you want to provision to monitor boot progress.

Procedure

1 Boot the remaining hosts.

   Auto Deploy boots the hosts, applies the host profile, and adds the hosts to the vCenter Server inventory. The hosts remain in maintenance mode because the host profile from the reference host is set up to require user input for each host.

2 Open a vSphere Client and connect to the vCenter Server system.

3 Click **Home** and select **Host Profiles**.

4 In the panel on the left, select the ESXiGold profile and add the newly booted hosts to that profile.

5 Apply the host profile to each of the hosts, provide the user input information, and reboot each host.

   When the reboot progress completes, all hosts are running with the image you specify and use the configuration in the reference host profile. The cluster shows that all hosts are fully compliant.

All hosts are now configured with the shared information through the reference host profile and with the host-specific information through the host customization mechanism. The next time you boot the hosts, they retrieve that information and boot completely.

What to do next

With your proof of concept implementation completed successfully, you can start planning your production setup.

Using vSphere ESXi Image Builder CLI 6

The ESXi Image Builder CLI is a set of PowerCLI cmdlets that you can use to manage vSphere image profiles and VIB packages, such as driver VIBs and update VIBs. You can also use Image Builder cmdlets to export an image profile to an ISO or offline depot ZIP file that you can use to install ESXi with a customized set of updates, patches, and drivers.

This chapter includes the following topics:

Understanding Image Builder

You can use the vSphere® ESXi™ Image Builder CLI to manage software depots, image profiles, and software packages (VIBs). Image profiles and VIBs specify the software you want to use during installation or upgrade of an ESXi host.

Image Builder Overview

The Image Builder PowerCLI supports management of vSphere image profiles and VIBs.

You can manage VIBs and image profiles with vSphere Image Builder. VIBs are software packages, and image profiles specify a set of software packages. See "Software Depots and Their Components," on page 146.

You use Image Builder cmdlets for managing the software to deploy to your ESXi hosts in several different scenarios.

Create image profiles for use by Auto Deploy. Use Image Builder to create an image profile that defines the VIBs that Auto Deploy uses to provision hosts.

Add custom third-party drivers to existing image profile and export to ISO or bundle. To add third-party driver or extension custom VIBs to your ESXi hosts, use Image builder to clone the base image provided by VMware, add the custom VIBs, and export to ISO or to offline bundle ZIP file.

Perform upgrades. If you upgrade from a 4.0 or 4.1 system that includes custom extensions or drivers, you can use Image Builder to create an image profile that includes the vSphere 5 base VIB. You can create vSphere 5 VIBs for the custom extensions and add those VIBs to the base VIB. Export the custom image profile to an ISO you can install or to a ZIP that you can use with vSphere Update Manager.

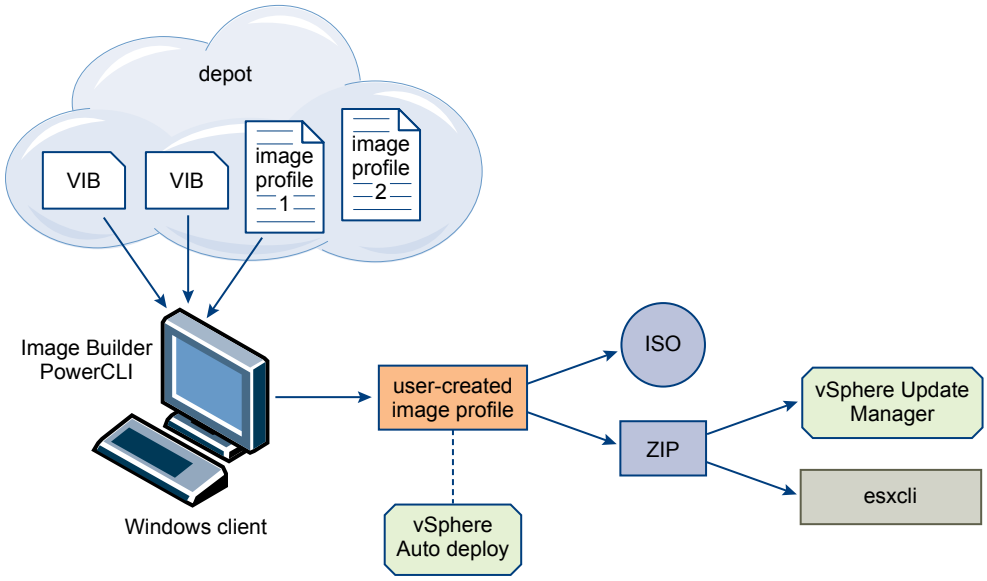
Create custom images with reduced footprint. Some customers require a minimal footprint image. These customers can clone the ESXi base image profile and remove VIBs using Image Builder.

The Image Builder PowerCLI cmdlets take image profiles and VIBs as input and produce different outputs.

Input. Image profiles and VIBs that are located in a software depot are used as input to PowerCLI cmdlets running on a Windows client.

Output. PowerCLI cmdlets create custom image profiles that can be exported to ISO or an offline depot ZIP file. ISO images are used for installation. The ZIP depot can be used by vSphere Update Manager or by `esxcli software` commands to update or install images. Image profiles are also used in vSphere Auto Deploy rules to specify the software to provision ESXi hosts with.

Figure 6-1. Image Builder Architecture



Software Depots and Their Components

Understanding how depots, profiles, and VIBs are structured and where you can use them is a prerequisite for in-memory installation of a custom ESXi ISO, for provisioning ESXi hosts using vSphere Auto Deploy, and for certain custom upgrade operations.

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.

See "SoftwarePackage Object Properties," on page 150.

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.

See "ImageProfile Object Properties," on page 149.

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.

Image Builder PowerCLI Overview

Image Builder PowerCLI cmdlets allow you to manage image profiles and VIBs.

The Image Builder PowerCLI includes the following cmdlets.

NOTE When you run Image Builder cmdlets, provide all parameters on the command line when you invoke the cmdlet. Supplying parameters in interactive mode is not recommended.

Run `Get-Help` *cmdlet_name* at the PowerCLI prompt for detailed reference information.

Table 6-1. Image Builder Cmdlets

Cmdlet	Description
`Add-EsxSoftwareDepot`	Adds the software depot or ZIP file at the specified location to your current environment. Downloads metadata from the depot and analyzes VIBs for dependencies.
`Remove-EsxSoftwareDepot`	Disconnects from the specified software depot.
`Get-EsxSoftwareDepot`	Returns a list of software depots that are in the current environment. If you want to examine and manage image profiles and VIBs, you must first add the corresponding software depot to your environment.
`Get-EsxSoftwarePackage`	Returns a list of software package objects (VIBs). Use this cmdlet's options to filter the results.
`Get-EsxImageProfile`	Returns an array of `ImageProfile` objects from all currently added depots.
`New-EsxImageProfile`	Creates a new image profile. In most cases, creating a new profile by cloning an existing profile is recommended. See "Create an Image Profile," on page 155.
`Set-EsxImageProfile`	Modifies a local `ImageProfile` object and performs validation tests on the modified profile. The cmdlet returns the modified object but does not persist it.
`Export-EsxImageProfile`	Exports an image profile as either an ESXi ISO image for ESXi installation, or as a ZIP file.
`Compare-EsxImageProfile`	Returns an `ImageProfileDiff` structure that shows whether the two profiles have the same VIB list and acceptance level. See "Acceptance Levels," on page 149.
`Remove-EsxImageProfile`	Removes the image profile from the software depot.
`Add-EsxSoftwarePackage`	Adds one or more new packages (VIBs) to an existing image profile.
`Remove-EsxSoftwarePackage`	Removes one or more packages (VIBs) from an image profile.

Image Profiles

Image profiles define the set of VIBs that an ESXi installation or update process uses. Image profiles apply to hosts provisioned with Auto Deploy and to other ESXi 5.x hosts. You define and manipulate image profiles with the Image Builder PowerCLI.

Image Profile Requirements

You can create a custom image profile from scratch or clone an existing profile and add or remove VIBs. A profile must meet the following requirements to be valid.

- Each image profile must have a unique name and vendor combination.
- Each image profile has an acceptance level. When you add a VIB to an image profile with an Image Builder PowerCLI cmdlet, Image Builder checks that the VIB matches the acceptance level defined for the profile.
- You cannot remove VIBs that are required by other VIBs.
- You cannot include two versions of the same VIB in an image profile. When you add a new version of a VIB, the new version replaces the existing version of the VIB.

Image Profile Validation

An image profile and its VIBs must meet several criteria to be valid.

- Image profiles must contain at least one base VIB and one bootable kernel module.
- If any VIB in the image profile depends on another VIB, that other VIB must also be included in the image profile. VIB creators store that information in the SoftwarePackage object's Depends property.
- VIBs must not conflict with each other. VIB creators store conflict information in the SoftwarePackage object's Conflicts property.
- Two VIBs with the same name, but two different versions, cannot coexist. When you add a new version of a VIB, the new version replaces the existing version of the VIB.
- No acceptance level validation issues exist.

When you make a change to an image profile, Image Builder checks that the change does not invalidate the profile.

Dependency Validation — When you add or remove a VIB, Image Builder checks that package dependencies are met. Each SoftwarePackage object includes a Depends property that specifies a list of other VIBs that VIB depends on. See "Structure of ImageProfile, SoftwarePackage, and ImageProfileDiff Objects," on page 149

Acceptance Level Validation — Image Builder performs acceptance level validation each time an image profile is created or changed. Image Builder checks the acceptance level of VIBs in the image profile against the minimum allowed acceptance level of the profile. The acceptance level of the VIB is also validated each time the signature of a VIB is validated.

VIB Validation During Export

When you export an image profile to an ISO, Image Builder validates each VIB by performing the following actions.

- Checks that no conflicts exist by checking the Conflicts property of each SoftwarePackage object.

- Performs VIB signature validation. Signature validation prevents unauthorized modification of VIB packages. The signature is a cryptographic checksum that guarantees that a VIB was produced by its author. Signature validation also happens during installation of VIBs on an ESXi host and when the Auto Deploy server uses VIBs.
- Checks that VIBs follow file path usage rules. VMware tests VMwareCertified and VMwareAccepted VIBs to guarantee those VIBs always follow file path usage rules.

Acceptance Levels

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. You can change the host acceptance levels with `esxcli` commands.

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.

Structure of ImageProfile, SoftwarePackage, and ImageProfileDiff Objects

In some situations, knowing the structure of `ImageProfile`, `SoftwarePackage`, and `ImageProfileDiff` objects helps you manage deployment and upgrade processes.

ImageProfile Object Properties

The `ImageProfile` object, which is accessible with the `Get-EsxImageProfile` PowerCLI cmdlet, has the following properties.

Name	Type	Description
AcceptanceLevel	AcceptanceLevel	Determines which VIBs you can add to the profile. Levels are VMwareCertified, VMwareAccepted, PartnerSupported, and CommunitySupported. See "Acceptance Levels," on page 149.
Author	System.String	Person who created the profile. 60 characters or fewer.
CreationTime	System.DateTime	Timestamp of creation time.
Description	System.String	Full text description of profile. No length limit.
GUID	System.String	Globally unique ID of the image profile.
ModifiedTime	System.DateTime	Timestamp of last modification time.
Name	System.String	Name of the image profile. 80 characters or fewer.
ReadOnly	System.Boolean	When set to true, the profile cannot be edited. Use `Set-EsxImageProfile -Readonly` to make your custom image profiles read only.
Rules	ImageProfileRule[]	Displays any OEM hardware requirements that the image profile might have. Auto Deploy checks this property when deploying an image profile and deploys the profile if matching hardware is available.
Vendor	System.String	Organization that publishes the profile. 40 characters or fewer.
VibList	SoftwarePackage[]	List of VIB IDs the image consists of.

SoftwarePackage Object Properties

When preparing an image profile, you can examine software packages to decide which packages are suitable for inclusion. The `SoftwarePackage` object has the following properties.

Name	Type	Description
AcceptanceLevel	AcceptanceLevel	Acceptance level of this VIB.
Conflicts	SoftwareConstraint[]	List of VIBs that cannot be installed at the same time as this VIB. Each constraint uses the following format: `package-name[<<|<=|=|>=|<< version]`
Depends	SoftwareConstraint[]	List of VIBs that must be installed at the same time as this VIB. Same constraint format as `Conflicts` property.
Description	System.String	Long description of the VIB.
Guid	System.String	Unique ID for the VIB.
LiveInstallOk	System.Boolean	True if live installs of this VIB are supported.
LiveRemoveOk	System.Boolean	True if live removals of this VIB are supported.

Name	Type	Description
MaintenanceMode	System.Boolean	True if hosts must be in maintenance mode for installation of this VIB.
Name	System.String	Name of the VIB. Usually uniquely describes the package on a running ESXi system.
Provides	SoftwareProvides	List of virtual packages or interfaces this VIB provides. See "SoftwareProvide Object Properties," on page 153.
ReferenceURLs	SupportReference[]	List of SupportReference objects with in-depth support information. The SupportReference object has two properties, Title and URL, both of type System.String.
Replaces	SoftwareConstraint[]	List of SoftwareConstraint objects that identify VIBs that repliace this VIB or make it obsolete. VIBs automatically replace VIBs with the same name but lower versions.
ReleaseDate	System.DateTime	Date and time of VIB publication or release.
SourceUrls	System.String[]	List of source URLs from which this VIB can be downloaded.
StatelessReady	System.Boolean	True if the package supports host profiles or other technologies that make it suitable for use in conjunction with vSphere Auto Deploy.
Summary	System.String	One-line summary of the VIB.
Tags	System.String[]	An array of string tags for this package defined by the vendor or publisher. Tags can be used to identify characteristics of a package.
Vendor	System.String	VIB vendor or publisher.
Version	System.String	VIB version.
VersionObject	Software.Version	The VersionObject property is of type SoftwareVersion. The SoftwareVersion class implements a static Compare method to compare two versions of strings. See "SoftwareVersion Object Properties," on page 152

ImageProfileDiff Object Properties

When you run the Compare-EsxImageProfile cmdlet, you pass in two parameters, first the reference profile, and then the comparison profile. The cmdlet returns an ImageProfileDiff object, which has the following properties.

Name	Type	Description
CompAcceptanceLevel	System.String	Acceptance level for the second profile that you passed to Compare-EsxImageProfile.
DowngradeFromRef	System.String[]	List of VIBs in the second profile that are downgrades from VIBs in the first profile.
Equal	System.Boolean	True if the two image profiles have identical packages and acceptance levels.
OnlyInComp	System.String	List of VIBs found only in the second profile that you passed to Compare-EsxImageProfile.
OnlyInRef	System.String[]	List of VIBs found only in the first profile that you passed to Compare-EsxImageProfile.
PackagesEqual	System.Boolean	True if the image profiles have identical sets of VIB packages.
RefAcceptanceLevel	System.String	Acceptance level for the first profile that you passed to Compare-EsxImageProfile.
UpgradeFromRef	System.String[]	List of VIBs in the second profile that are upgrades from VIBs in the first profile.

SoftwareVersion Object Properties

The SoftwareVersion object allows you to compare two version strings. The object includes a Compare static methot that accepts two strings as input and returns 1 if the first version string is higher than the second version string. Compare returns 0 if two versions strings are equal. Compare returns -1 if the second version string is higher than the first string. The object has the following properties.

Name	Type	Description
Version	System.String	The part of the version before the hyphen. This part indicates the primary version.
Release	System.String	The part of the version after the hyphen. This part indicates the release version.

SoftwareConstraint Object Properties

The SoftwareConstraint object implements a MatchesProvide method. The method accepts a SoftwareProvides or SoftwarePackage object as input and returns True if the constraint matches the SoftwareProvide or the SoftwarePackage, or False otherwise.

The SoftwareConstraint object also includes the following properties.

Name	Type	Description
Name	System.String	Name of the constraint. This name should match a corresponding SoftwareProvides Name property.
Relation	System.String	An enum, or one of the following comparison indicators: <<, <=, = >=, >>. This property can be $null if the constraint does not have a Relation and Version property.
Version	System.String	The version to match the constraint against. This property can be $null if the constraint does not have a Relation and Version property.
VersionObject	SoftwareVersion	The version represented by a SoftwareVersion object.

SoftwareProvide Object Properties

The SoftwareProvide object includes the following properties.

Name	Type	Description
Name	System.String	Name of the provide
Version	System.String	Version of the provide. Can be $null if the provide does not specify a version.
Release	System.String	Version of the provide as represented by a SoftwareVersion object. See "SoftwareVersion Object Properties," on page 152.

Image Builder Installation and Usage

Image Builder consists of the Image Builder server and the Image Builder PowerShell cmdlets. The Image Builder server starts when your run the first Image Builder cmdlet.

Install Image Builder PowerCLI and Prerequisite Software

Before you can run Image Builder cmdlets, you must install vSphere PowerCLI and all prerequisite software. The Image Builder snap-in is included with the PowerCLI installation.

You install Image Builder and prerequisite software on a Microsoft Windows system.

Procedure

1 Install Microsoft .NET 2.0 from the Microsoft website following the instructions on that website.

2 Install Microsoft PowerShell 2.0. from the Microsoft website following the instructions on that website.

3 Install vSphere PowerCLI, which includes the Image Builder cmdlets.

  See the *vSphere PowerCLI Installation Guide* for detailed instructions.

What to do next

Review "Using Image Builder Cmdlets," on page 154.If you are new to PowerCLI, read the PowerCLI documentation.

Use Image Builder cmdlets and other PowerCLI cmdlets and PowerShell cmdlets to manage image profiles and VIBs. Use `Get-Help` *cmdlet_name* at any time for command-line help.

Using Image Builder Cmdlets

Image Builder cmdlets are implemented as Microsoft PowerShell cmdlets and included in VMware PowerCLI. Users of Image Builder cmdlets can take advantage of all PowerCLI features.

Experienced PowerShell users can use Image Builder cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and PowerCLI, the following tips help you come up to speed.

You can type cmdlets, parameters, and parameter values in the PowerCLI shell.

- Get help for any cmdlet by running **`Get-Help`** ***`cmdlet_name`***.
- Remember that PowerShell is not case sensitive.
- Use tab completion for cmdlet names and parameter names.
- Format any variable and cmdlet output by using **`Format-List`** or **`Format-Table`** or their short forms **`fl`** or **`ft`**. See **`Get-Help Format-List`**.

Passing Parameters by Name

You can pass in parameters by name in most cases and surround parameter values that contain spaces or special characters with double quotes.

```
Add-EsxSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Passing Parameters as Objects

You can pass parameters as objects if you want to do scripting and automation. You can use the technique with cmdlets that return multiple objects or with cmdlets that return a single object.

1 Bind the output of a cmdlet that returns multiple objects to a variable.

```
$profs = Get-EsxImageProfile
```

2 When you run the cmdlet that needs the object as input, access the object by position, with the list starting with 0.

```
Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
```

The example adds the specified software package to the fifth image profile in the list returned by `Get-EsxImageProfile`.

Most examples in the documentation pass in parameters by name. "Image Builder Workflows," on page 161 includes examples that pass parameters as objects.

Setting Properties to Support Remote Signing

For security reasons, Windows PowerShell supports an execution policy feature. It determines whether scripts are allowed to run and whether they must be digitally signed. By default, the execution policy is set to Restricted, which is the most secure policy. If you want to run scripts or load configuration files, you can change the execution policy by using the `Set-ExecutionPolicy` cmdlet. To do this, type the following in the vSphere PowerCLI console window.

```
Set-ExecutionPolicy RemoteSigned
```

If the command is successful, you can run scripts and load configuration files. For more information about the execution policy and digital signing in Windows PowerShell, use the following cmdlet.

```
Get-Help About_Signing
```

Image Builder Common Tasks

The Image Builder PowerCLI cmdlets allow you to manipulate software depots, image profiles, and VIBs.

Create an Image Profile

Cloning a published profile is the easiest way to create a custom image profile. Cloning a profile is especially useful if you want to remove a few VIBs from a profile, or if you want to use hosts from different vendors and want to use the same basic profile, but want to add vendor-specific VIBs. VMware partners or large installations might consider creating a profile from scratch.

Administrators performing this task must have some experience with PowerCLI or Microsoft PowerShell.

Prerequisites

- Install the VMware PowerCLI and all prerequisite software. See "Image Builder Installation and Usage," on page 153.
- Verify that you have access to the software depot that contains the image profile you want to clone.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Procedure

1 At the PowerShell prompt, add the depot that contains the profile you want to clone to the current session.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot -DepotUrl`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path. b Run **`Add-EsxSoftwareDepot -DepotUrl C:\`*`file_path`*`\`*`offline-bundle`*`.zip`**

The cmdlet returns one or more `SoftwareDepot` objects.

2 (Optional) Run the `Get-EsxImageProfile` cmdlet to find the name of the profile that you want to clone.

```
Get-ESXImageProfile
```

You can use filtering options with `Get-EsxImageProfile`.

3 Run the `New-EsxImageProfile` cmdlet to create the new profile and use the `-CloneProfile` parameter to specify the profile you want to clone.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
```

This example clones the profile named `My-Profile` and assigns it the name `Test Profile 42`. You must specify a unique combination of name and vendor for the cloned profile.

What to do next

See "Examining Depot Contents," on page 161 for some examples of filtering.

Customize the image profile by adding or removing VIBs. See "Add VIBs to an Image Profile," on page 156.

Add VIBs to an Image Profile

You can add one or more VIBs to an image profile if that image profile is not set to ReadOnly. If the new VIB depends on other VIBs or conflicts with other VIBs in the profile, a message is displayed at the PowerShell prompt and the VIB is not added.

You can add VIBs from VMware or from VMware partners to an image profile. If you add VMware VIBs, the Image Builder PowerCLI performs validation. If you add VIBs from two or more OEM partners, no errors are reported but the resulting image profile might not work. Install VIBs from only one OEM vendor at a time.

NOTE You might be able to add VIBs even if the resulting image profile is invalid.

Administrators performing this task must have some experience with PowerCLI or Microsoft PowerShell.

Prerequisites

- Install the VMware PowerCLI and all prerequisite software. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Procedure

1 Run `Add-EsxSoftwareDepot` for each depot you want to work with.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot -DepotUrl`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path. b Run **`Add-EsxSoftwareDepot -DepotUrl C:\`*`file_path`*`\`*`offline-bundle`*`.zip`**

The cmdlet returns one or more `SoftwareDepot` objects.

2 Run `Get-EsxImageProfile` to list all image profiles in all currently visible depots.

```
Get-EsxImageProfile
```

The cmdlet returns all available profiles. You can narrow your search by using the optional arguments to filter the output.

3 Clone the profile.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
```

Image profiles published by VMware and its partners are read only. To make changes, you clone the image profile. The `vendor` parameter is required.

4 Run `Add-EsxSoftwarePackage` to add a new package to one of the image profile.

```
Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
```

The cmdlet runs the standard validation tests on the image profile. If validation succeeds, the cmdlet returns a modified, validated image profile. If the VIB that you want to add depends on a different VIB, the cmdlet displays that information and includes the VIB that would resolve the dependency. If the acceptance level of the VIB that you want to add is lower than the image profile acceptance level, an error results. Change the acceptance level of the image profile to add the VIB.

5 (Optional) Change the acceptance level of the image profile if an error about acceptance level problems displays.

VIB acceptance levels are set during VIB creation and cannot be changed.

The image profile includes the new VIB.

Export an Image Profile to ISO or Offline Bundle ZIP

You can export an image profile to an ISO image or a ZIP file of component files and folders. You cannot create both by running the cmdlet once. You can use the ISO image as an ESXi installer or upload the ISO into vSphere Update Manager for upgrades. You can use the ZIP file, which contains metadata and the VIBs specified in the image profile, for upgrades to ESXi 5.0 and later.

Administrators performing this task must have some experience with PowerCLI or Microsoft PowerShell.

Prerequisites

- Install the VMware PowerCLI and all prerequisite software. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Procedure

1 Run `Add-EsxSoftwareDepot` to connect to the depot that contains the image profile to export.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot -DepotUrl`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path. b Run **`Add-EsxSoftwareDepot -DepotUrl C:\`*`file_path`*`\`*`offline-bundle`*`.zip`**

The cmdlet returns one or more `SoftwareDepot` objects.

2 Run `Export-EsxImageProfile` to export the image profile.

To build...	Run...
ISO images	`Export-EsxImageProfile` with the `-ExportToIso` parameter.
Offline depot ZIP files	`Export-EsxImageProfile` with the `-ExportToBundle` parameter.

For the ISO image, Image Builder validates VIB signatures, adds VIB binaries to the image, and downloads the image to the specified location. For the ZIP file, Image Builder validates VIB signatures and downloads the VIB binaries to the specified location.

Example: Exporting an Image Profile to ISO or Offline Bundle

Export an image profile to ISO from the PowerCLI prompt.

1 Add the software depot.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Display all available image profiles to find the name of the image profile to export.

```
Get-EsxImageProfile
```

3 Export the image profile.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
```

Export an image profile to an offline bundle ZIP from the PowerCLI prompt.

1 Add the software depot.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Display all available image profiles to find the name of the image profile to export.

```
Get-EsxImageProfile
```

3 Export the image profile.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
```

What to do next

Use the ISO image in an ESXi installation or upload the ISO image into vSphere Update Manager to perform upgrades.

Use the ZIP file to upgrade an ESXi installation.

- Import the ZIP file into vSphere Update Manager for use with patch baselines.
- Download the ZIP file to an ESXi host or a datastore and run `esxcli software vib` commands to import the VIBs in the ZIP file.

See the *vSphere Upgrade* documentation.

Preserve Image Profiles Across Sessions

When you create an image profile and exit the PowerCLI session, the image profile is no longer available when you start a new session. You can export the image profile to a ZIP file software depot, and add that depot in the next session.

Prerequisites

- Install the VMware PowerCLI and all prerequisite software. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Procedure

1 In a PowerCLI session, create an image profile, for example by cloning an existing image profile and adding a VIB.

2 Before you exit the session, export the image profile to a ZIP file by calling `Export-EsxImageProfile` with the `ExportToBundle` parameter.

```
Export-EsxImageProfile -ImageProfile "my_profile" -ExportToBundle -FilePath "C:\isos\temp-base-plus-vib25.zip"
```

3 Exit the PowerCLI session.

4 When you start a new PowerCLI session, you can add the depot to access your image profile.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Working with Acceptance Levels

Hosts, image profiles, and individual VIBs have acceptance levels. VIB acceptance levels show tested the VIB. Understanding what each acceptance level implies, how to change levels, and what a change implies is an important part of installation and update procedures.

Acceptance levels are set for hosts, image profiles, and individual VIBs. The default acceptance level for an ESXi image or image profile is PartnerSupported.

Host acceptance levels

The host acceptance level determines which VIBs you can install on a host. You can change a host's acceptance level with ESXCLI commands. By default, ESXi hosts have an acceptance level of PartnerSupported to allow for easy updates with PartnerSupported VIBs.

NOTE VMware supports hosts at the PartnerSupported acceptance level. For problems with individual VIBs with PartnerSupported acceptance level, VMware refers you to the partner's support organization.

.

Image profile acceptance levels

The image profile acceptance level is set to the lowest VIB acceptance level in the image profile. If you want to add a VIB with a low acceptance level to an image profile, you can change the image profile acceptance level with the `Set-EsxImageProfile` cmdlet. See "Set the Image Profile Acceptance Level," on page 161.

The vSphere Update Manager does not display the actual acceptance level. Use Image Builder PowerCLI cmdlets to retrieve the acceptance level information for VIBs and image profiles.

VIB acceptance levels

A VIB's acceptance level is set when the VIB is created. Only the VIB creator can set the acceptance level.

If you attempt to provision a host with an image profile or VIB that has a lower acceptance level than the host, an error results. Change the acceptance level of the host to install the image profile or VIB. See "Change the Host Acceptance Level," on page 160. Changing the acceptance level of the host changes the system support for that host.

The acceptance level of a host, image profile, or VIB allows you to determine who tested the VIB and who supports the VIB. 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.

Change the Host Acceptance Level

You can lower the host acceptance level to match the acceptance level for a VIB or image profile you want to install.

The acceptance level of each VIB on a host must be at least as high as the host acceptance level. For example, you cannot install a VIB with PartnerSupported acceptance level on a host with VMwareAccepted acceptance level. You must first lower the acceptance level of the host.

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 Get the host acceptance level.

```
esxcli --server=server_name software acceptance get
```

3 If the acceptance level of the VIB is lower 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 value for *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

NOTE If the host has a higher acceptance level than the VIB or image profile you want to add, you can run commands in the `esxcli software vib` or `esxcli software profile` namespace with the `--force` option. When you use the `--force` option, a warning appears 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 that has inconsistent acceptance levels.

Set the Image Profile Acceptance Level

If you want to add a VIB to an image profile, and the VIB acceptance level is lower than the image profile acceptance level, you can clone the image profile with a lower acceptance level or change the image profile acceptance level.

Prerequisites

- Install the VMware PowerCLI and all prerequisite software. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Procedure

1 Run `Add-EsxSoftwareDepot` for each depot you want to work with.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot -DepotUrl`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path. b Run **`Add-EsxSoftwareDepot -DepotUrl C:\`*`file_path`*`\`*`offline-bundle`*`.zip`**.

2 Get the acceptance level for the image profile.

```
Get-EsxImageProfile -Name string
```

3 Set the acceptance level of the image profile.

```
Set-EsxImageProfile -Name string -AcceptanceLevel level
```

You can specify VMwareCertified, VMwareAccepted, PartnerSupported, or CommunitySupported as an acceptance level. If you lower the acceptance level, the level of support for the image profile and hosts that you provision with it changes. See "Acceptance Levels," on page 149.

Image Builder Workflows

Image Builder workflows are examples for cmdlet usage. Workflows do not represent actual tasks, but illustrate how you might explore different ways of using a cmdlet. Administrators trying out the workflows benefit from some experience with PowerCLI, Microsoft PowerShell, or both.

Examining Depot Contents

You can examine software depots and VIBs with Image Builder PowerCLI cmdlets. This workflow illustrates examining depot contents and includes examples of wildcard usage.

The workflow itself passes parameters by name, the example below passes parameters as objects by accessing variables.

Before you use the cmdlets in this workflow, make sure your environment meets the following requirements.

- VMware PowerCLI and prerequisite is software installed. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Examining depot contents is facilitated by the use of filtering options and wildcard characters.

1 At the PowerShell prompt, add the depot that you want to examine to the current session.

For remote depots, run **Add-EsxSoftwareDepot -DepotUrl *depot_url***.

For an offline depot ZIP file, you must download the ZIP file first.

a Download the ZIP file to a local file path, but do not unzip it.

b Run **Add-EsxSoftwareDepot -DepotUrl C:*file_path**offline-bundle*.zip**

2 Retrieve image profiles.

You can filter by vendor, name and acceptance level.

- **Get-EsxImageProfiles**

  Returns an array of `ImageProfile` objects from all depots you added to the session.

- **Get-EsxImageProfile -Vendor "C*"**

  Returns all image profiles create by a vendor with a name that starts with a `C`.

3 Retrieve software packages by using `Get-EsxSoftwarePackage`.

You can filter, for example by vendor or version, and you can use the standard PowerShell wildcard characters.

- **Get-EsxSoftwarePackage -Vendor "V*"**

  Returns all software packages from a vendor with a name that starts with a `V`.

- **Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"**

  Returns all software packages with a name that has the string `scsi` in it from a vendor with a name that starts with a `V`.

- **Get-EsxSoftwarePackage -Version "2.0*"**

  Returns all software packages with a version string that starts with a `2.0`.

4 Use `-Newest` to find the newest package.

- **Get-EsxSoftwarePackage -Vendor "V*" -Newest**

  Returns the newest package for the vendors starting with V and displays the information as a table.

- **Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list**

  Pipes the output of the request for software packages to the PowerShell `format-list` cmdlet and displays detailed information about each software package.

5 Display the list of VIBs in the image profile.

```
(Get-EsxImageProfile -Name "Robin's Profile").VibList
```

`VibList` is a property of the `ImageProfile` object. See "Structure of ImageProfile, SoftwarePackage, and ImageProfileDiff Objects," on page 149.

6 Retrieve software packages released before or after a certain date by using the `CreatedBefore` or `CreatedAfter` parameter.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Example: Depot Content Examination Using Variables

This example workflow examines depot contents by passing in parameters as objects, accessed by position in a variable, instead of passing in parameters by name. You can run the following commands in sequence from the PowerCLI prompt. Replace names with names that are appropriate in your installation.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Creating Image Profiles by Cloning Workflow

You can use Image Builder cmdlets to check which depots are available, to add a depot, to display image profile information, and to create a new image profile by cloning one of the available image profiles.

Before you use the cmdlets in this workflow, make sure your environment meets the following requirements.

- VMware PowerCLI and prerequisite is software installed. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See "Using Image Builder Cmdlets," on page 154.

Published profiles are usually read only and cannot be modified. Even if a published profile is not read only, cloning instead of modifying the profile is a best practice, because modifying the original profile erases the original. You cannot revert to the original, unmodified profile except by reconnecting to a depot.

A profile cloning workflow might include checking the current state of the system, adding a software depot, and cloning the profile.

1 In a PowerShell window, check whether any software depots are defined for the current session.

```
$DefaultSoftwareDepots
```

PowerShell returns the currently defined depots, or nothing if you just started PowerShell.

2 If necessary, add the depot that includes the profile you want to clone to the current session.

For remote depots, run **Add-EsxSoftwareDepot -DepotUrl *depot_url***.

For an offline depot ZIP file, you must download the ZIP file first.

a Download the ZIP file to a local file path.

b Run **Add-EsxSoftwareDepot -DepotUrl C:*file_path**offline-bundle*.zip**

PowerShell adds the specified depot to your current session and lists all current depots.

3 Check the `$DefaultSoftwareDepots` variable, which now returns the newly-added depot.

```
$DefaultSoftwareDepots
```

4 Display all currently available image profiles.

```
Get-EsxImageProfile
```

The list helps you pick a likely candidate for cloning.

5 Clone one of the image profiles by specifying the name displayed in the Name column, a name for the new profile, and the vendor.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor "Vendor20"
```

6 Display the newly created image profile.

```
$ip

Name                Vendor          Last Modified          Acceptance Level
----                ------          -------------          ----------------
Test Profile 42     Vendor20        9/15/2010 5:45:43...   PartnerSupported
```

Example: Creating Image Profile by Cloning Using Variables

This sample cmdlet sequence repeats the steps of this workflow, but passes parameters as objects, accessed by position in a variable, instead of passing parameters by name. You can run the following cmdlets in sequence from the PowerCLI prompt.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Creating Image Profiles from Scratch Workflow

In most situations, you create an image profile by cloning an existing profile. Some VMware customers or partners might need to create an image profile from scratch. Pay careful attention to dependencies and acceptance levels if you create an image profile from scratch.

Before you use the cmdlets in this workflow, make sure your environment meets the following requirements.

- VMware PowerCLI and prerequisite is software installed. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- You have access to a depot that includes a base image and one or more VIBs. VMware and VMware partners make public depots, accessible by a URL, available. VMware or VMware partners can create a ZIP file that you can unzip to your local environment and access by using a file path.

See "Create an Image Profile," on page 155 for an example of cloning and modifying an image profile.

The system expects that the acceptance level of the VIBs you add to the base image is at least as high as the level of the base image. Pass in the `-AcceptanceLevel` parameter to change the acceptance level of the image profile if you have to add a VIB with a lower acceptance level.

As an alternative to specifying the parameters on the command line, you can use the PowerShell prompting mechanism to specify string parameters. Prompting does not work for other parameters such as objects.

The following workflow illustrates creating image profiles from scratch.

1 At the PowerShell prompt, add the depot that contains the packages you want to use to the current session.

   For remote depots, run **`Add-EsxSoftwareDepot -DepotUrl depot_url`**.

   For an offline depot ZIP file, you must download the ZIP file first.

   a Download the ZIP file to a local file path.

   b Run **`Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip`**

2 List the available packages that you are interested in and bind them to a variable.

   `Get-EsxSoftwarePackage -CreatedAfter 7/1/2010`

3 Create a new profile, assign it a name and vendor, and add a base package.

   `New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-base[0]`

   The example uses the esx-base package. In most cases, you include the esx-base package when you create an image profile from scratch. Names that contain spaces are surrounded by quotes.

4 Pipe the information about the new image profile to `format-list` for detailed information about the new package.

```
(Get-EsxImageProfile -Name "Test #2").VibList | format-list
```

Example: Creating Image Profiles from Scratch Using Variables

This command sequence repeats the steps of the workflow, but passes parameters as objects, accessed by position in a variable, instead of passing parameters by name. You can run the following commands in sequence from the PowerCLI prompt.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage $pkgs[0]
$ip2 | format-list
```

Editing Image Profiles Workflow

You can create a custom image by cloning and editing an image profile. You can add or replace one or more VIBs in the existing profile. If adding or replacing VIBs would make the image profile inconsistent, an error results.

Before you use the cmdlets in this workflow, make sure your environment meets the following requirements.

- VMware PowerCLI and prerequisite is software installed. See "Install Image Builder PowerCLI and Prerequisite Software," on page 153.
- You have access to a depot that includes a base image and one or more VIBs. VMware and VMware partners make public depots, accessible by a URL, available. VMware or VMware partners can create a ZIP file that you can download to your local environment and access by using a file path.

1 At the PowerShell prompt, add the depot that contains the image profile that you want to edit to the current session.

   For remote depots, run **`Add-EsxSoftwareDepot -DepotUrl depot_url`**.

   For an offline depot ZIP file, you must download the ZIP file first.

   a Download the ZIP file to a local file path.

   b Run **`Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip`**

2 Pipe the image profile you intend to edit to `format-list` to see detailed information. In this example, the image profile created in "Creating Image Profiles from Scratch Workflow," on page 164 contains only the base image. A newly created image profile is not included in the depot. Instead, you access the image profile by name or by binding it to a variable.

   ```
   Get-EsxImageProfile "Test #2" | format-list
   ```

   PowerShell returns the formatted information.

   ```
   Name            : Test #2
   Vendor           : Vendor42
   ...
   VibList          : {esx-base 5.0.0.-...,}
   ```

3 (Optional) If you are adding a VIB with a lower acceptance level than the image profile's level, change the acceptance level of the image profile.

```
Set-EsxImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
```

PowerShell returns the information about the changed profile in tabular format.

```
Name           Vendor          Last Modified       Acceptance Level
----           ------          -------------       ----------------
Test #2        Vendor42        9/22/2010 12:05:... VMwareAccepted
```

4 Add a software package (VIB) to the image profile. You can add the package by name.

```
Add-EsxSoftwarePackage -ImageProfile "Test #2" -SoftwarePackage NewPack3
```

PowerShell returns the information about the image profile in tabular format.

```
Name           Vendor          Last Modified       Acceptance Level
----           ------          -------------       ----------------
Test #2        Vendor42        9/22/2010 12:05:... VMwareAccepted
```

5 Display the image profile again.

```
Get-EsxImageProfile "Test #2" | format-list
```

The VIB list is updated to include the new software package and the information is displayed.

```
Name            : Test #2
Vendor           : Vendor42
...
VibList          : {esx-base 5.0.0.-..., NewPack3}
```

Example: Editing Image Profiles with Variables

This cmdlet sequence repeats the steps of the workflow but passes parameters as objects, accessed by position in a variable, instead of passing parameters by name. You can run the following cmdlets in sequence from the PowerCLI prompt.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Setting Up ESXi 7

These topics provide information about using the direct console user interface and configuring defaults for ESXi.

This chapter includes the following topics:

ESXi Autoconfiguration

When you turn on the ESXi host for the first time or after resetting the configuration defaults, the host enters an autoconfiguration phase. This phase configures system network and storage devices with default settings.

By default, Dynamic Host Configuration Protocol (DHCP) configures IP, and all visible blank internal disks are formatted with the virtual machine file system (VMFS) so that virtual machines can be stored on the disks.

About the Direct Console ESXi Interface

Use the direct console interface for initial ESXi configuration and troubleshooting.

Connect a keyboard and monitor to the host to use the direct console. After the host completes the autoconfiguration phase, the direct console appears on the monitor. You can examine the default network configuration and change any settings that are not compatible with your network environment.

Key operations available to you in the direct console include:

- Configuring hosts
- Setting up administrative access
- Troubleshooting

You can also use vSphere client applications to manage the host.

Table 7-1. Navigating in the Direct Console

Action	Key
View and change the configuration	F2
Change the user interface to high-contrast mode	F4
Shut down or restart the host	F12
Move the selection between fields	Arrow keys
Select a menu item	Enter
Toggle a value	Spacebar
Confirm sensitive commands, such as resetting configuration defaults	F11
Save and exit	Enter
Exit without saving	Esc
Exit system logs	q

Configure the Keyboard Layout for the Direct Console

You can configure the layout for the keyboard that you use with the direct console.

Procedure

1 From the direct console, select **Configure Keyboard** and press Enter.

2 Select the layout to use.

3 Press the spacebar to toggle selections on and off.

4 Press Enter.

Create a Security Banner for the Direct Console

A security banner is a message that is displayed on the direct console Welcome screen.

Procedure

1 Log in to the host from the vSphere Client.

2 From the **Configuration** tab, select **Advanced Settings**.

3 From the Advanced Settings window, select **Annotations**.

4 Enter a security message.

The message is displayed on the direct console Welcome screen.

Redirecting the Direct Console to a Serial Port

To manage your ESXi host remotely from a serial console, you can redirect the direct console to a serial port.

vSphere supports the VT100 terminal type and the PuTTy terminal emulator to view the direct console over the serial port.

You can redirect the direct console to a serial port in several ways.

- Redirect the Direct Console to a Serial Port by Setting the Boot Options Manually on page 169

  When you redirect the direct console to a serial port by setting the boot options, the change does not persist for subsequent boots.

- Redirect the Direct Console to a Serial Port by Using the vSphere Client on page 170

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

- Redirect the Direct Console to a Serial Port from the vSphere Web Client on page 170

  You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Web Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

- Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy on page 171

  After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

Redirect the Direct Console to a Serial Port by Setting the Boot Options Manually

When you redirect the direct console to a serial port by setting the boot options, the change does not persist for subsequent boots.

Prerequisites

Verify that the serial port is not in use for serial logging and debugging.

Procedure

1 Start the host.

2 When the Loading VMware Hypervisor window appears, press Shift+O to edit boot options.

3 Disable the logPort and gdbPort on com1 and set tty2Port to com1 by entering the following boot options:

```
"gdbPort=none logPort=none tty2Port=com1";
```

To use com2 instead, replace `com1` with `com2`.

The direct console is redirected to the serial port until you reboot the host. To redirect the direct console for subsequent boots, see "Redirect the Direct Console to a Serial Port by Using the vSphere Client," on page 170

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

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

Prerequisites

- Verify that you can access the host from the vSphere Client.
- Verify that the serial port is not already be in use for serial logging and debugging, or for ESX Shell (tty1Port).

Procedure

1 From the vSphere Client, connect to the vCenter Server and select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, click **Advanced Settings**.

4 In the left pane, expand the **VMkernel** listing and select **Boot**.

5 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.

6 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: **`com1`** or **`com2.`**

7 Click **OK**.

8 Reboot the host.

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

Redirect the Direct Console to a Serial Port from the vSphere Web Client

You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Web Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

Prerequisites

- Verify that you can access the host from the vSphere Client.
- Verify that the serial port is not in use for serial logging and debugging, or for ESX Shell (tty1Port).

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Click the **Manage** tab.

4 Select **Settings**.

5 Select **Advanced System Settings**.

6 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.

7 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: **`com1`** or **`com2.`**

8 Reboot the host.

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

Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy

After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

Prerequisites

The serial port must not already be in use for serial logging and debugging.

Procedure

1 From the vSphere Client, connect to the vCenter Server and select the host in the inventory.

2 Click the **Configuration** tab.

3 Under Software, click **Advanced Settings**.

4 In the left pane, expand the **VMkernel** listing and select **Boot**.

5 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.

6 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: **`com1`** or **`com2.`**

7 Click **OK**.

8 Save the host profile and attach the host to the profile. See the *vSphere Host Profiles* documentation.

The setting to redirect the direct console to a serial port is stored by vCenter Server and persists when you reprovision the host with Auto Deploy.

Set the Password for the Administrator Account

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

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

Procedure

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

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

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

4 Retype the new password and press Enter.

Configuring the BIOS Boot Settings

If your server has multiple drives, you might need to configure the BIOS settings.

The BIOS boot configuration determines how your server boots. Generally, the CD-ROM device is listed first.

NOTE If you are using ESXi Embedded, the BIOS boot configuration determines whether your server boots into the ESXi boot device or another boot device. Generally, the USB flash device is listed first in the BIOS boot settings on the machine that hosts ESXi.

You can change the boot setting by configuring the boot order in the BIOS during startup or by selecting a boot device from the boot device selection menu. When you change the boot order in the BIOS, the new setting affects all subsequent reboots. When you select a boot device from the boot device selection menu, the selection affects the current boot only.

Some servers do not have a boot device selection menu, in which case you must change the boot order in the BIOS even for one-time boots, and then change it back again during a subsequent reboot.

NOTE The boot device selection menu is different from the system boot options that you can configure in the vSphere Client.

With the vSphere Client boot options, you can configure the boot sequence for floppy, CD-ROM, and hard disk drives only. For some servers, the system BIOS has two options. One is for the boot sequence (floppy, CD-ROM, hard disk) and another for the hard disk boot order (USB key, local hard disk). When you are using the vSphere Client, the boot options correspond to the BIOS boot sequence (floppy, CD-ROM, hard disk).

Change the BIOS Boot Setting for ESXi

Configure the BIOS boot setting for ESXi if you want the server to boot into ESXi by default.

ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1 While the ESXi host is powering on, press the key required to enter your host's BIOS setup.

Depending on your server hardware, the key might be a function key or Delete. The option to enter the BIOS setup might be different for your server.

2 Select the BIOS boot setting.

Option	Description
If you are using the installable version of ESXi	Select the disk on which you installed the ESXi software and move it to the first position in the list. The host boots into ESXi.
If you are using ESXi Embedded	Select the USB flash device and move it to the first position in the list. The host starts in ESXi mode.

Configure the Boot Setting for Virtual Media

If you are using remote management software to set up ESXi, you might need to configure the boot setting for virtual media.

Virtual media is a method of connecting a remote storage media such as CD-ROM, USB mass storage, ISO image, and floppy disk to a target server that can be anywhere on the network. The target server has access to the remote media, and can read from and write to it as if it were physically connected to the server's USB port.

Prerequisites

ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1 Connect the media to the virtual device.

   For example, if you are using a Dell server, log in to the Dell Remote Access Controller (DRAC) or a similar remote management interface and select a physical floppy or CD-ROM drive, or provide a path to a floppy image or CD-ROM image.

2 Reboot the server.

3 While the server is powering on, enter the device selection menu.

   Depending on your server hardware, the key might be a function key or Delete.

4 Follow the instructions to select the virtual device.

The server boots from the configured device once and goes back to the default boot order for subsequent boots.

Host Fails to Boot After You Install ESXi in UEFI Mode

When you install ESXi on a host machine in UEFI mode, the machine might fail to boot.

Problem

When you reboot after installing ESXi on a host machine in UEFI mode, the reboot might fail. This problem is accompanied by an error message similar to `Unexpected network error. No boot device available.`

Cause

The host system fails to recognize the disk that ESXi is installed on as the boot disk.

Solution

1 While the error message is displayed on screen, press F11 to display boot options.

2 Select an option similar to **Add boot option**.

   The wording of the option might vary, depending on your system.

3 Select the file `\EFI\BOOT\BOOTx64.EFI` on the disk that you installed ESXi on.

4 Change the boot order so that the host boots from the option that you added.

Network Access to Your ESXi Host

The default behavior is to configure the ESXi management network using DHCP. You can override the default behavior and use static IP settings for the management network after the installation is completed.

Table 7-2. Network Configuration Scenarios Supported by ESXi

Scenario	Approach
You want to accept the DHCP-configured IP settings.	In the ESXi direct console, you can find the IP address assigned through DHCP to the ESXi management interface. You can use that IP address to connect to the host from the vSphere Client and customize settings, including changing the management IP address.
One of the following is true: ■ You do not have a DHCP server. ■ The ESXi host is not connected to a DHCP server. ■ Your connected DHCP server is not functioning properly.	During the autoconfiguration phase, the software assigns the link local IP address, which is in the subnet 169.254.x.x/16. The assigned IP address appears on the direct console. You can override the link local IP address by configuring a static IP address using the direct console.

Table 7-2. Network Configuration Scenarios Supported by ESXi (Continued)

Scenario	Approach
The ESXi host is connected to a functioning DHCP server, but you do not want to use the DHCP-configured IP address.	During the autoconfiguration phase, the software assigns a DHCP-configured IP address. You can make the initial connection by using the DHCP-configured IP address. Then you can configure a static IP address. If you have physical access to the ESXi host, you can override the DHCP-configured IP address by configuring a static IP address using the direct console.
Your security deployment policies do not permit unconfigured hosts to be powered on the network.	Follow the setup procedure in "Configure the Network Settings on a Host That Is Not Attached to the Network," on page 174.

Configure the Network Settings on a Host That Is Not Attached to the Network

Some highly secure environments do not permit unconfigured hosts on the network to be powered on. You can configure the host before you attach the host to the network.

Prerequisites

Verify that no network cables are connected to the host.

Procedure

1 Power on the host.

2 Use the direct console to configure the password for the administrator account (root).

3 Use the direct console to configure a static IP address.

4 Connect a network cable to the host.

5 (Optional) Use the vSphere Client or the vSphere Web Clientto connect to a vCenter Server system.

6 (Optional) Add the host to the vCenter Server inventory.

Managing ESXi Remotely

You can use the vSphere Client, the vSphere Web Client, and vCenter Server to manage the host.

To manage the host with the vSphere Client, the vSphere Web Client, and vCenter Server, the applications must be installed on a computer that serves as a management station with network access to the ESXi host. The ESXi host must be powered on. For instructions about downloading and installing vCenter Server, the vSphere Client, and the vSphere Web Client, see the following topics.

- "Download the vCenter Server Installer," on page 246
- "Install vCenter Server in a Separate Installation," on page 268
- "Download the vSphere Client," on page 280
- "Install the vSphere Client," on page 280
- "Install or Upgrade the vSphere Web Client," on page 282

Configuring Network Settings

ESXi requires one IP address for the management network. To configure basic network settings, use the vSphere Client or the direct console.

Use the vSphere Client in the following cases:

- You are satisfied with the IP address assigned by the DHCP server.
- You are allowed to temporarily use the IP address assigned by the DHCP server. In this case, connect to that address with the vSphere Client, and use the vSphere Client to assign a static IP address.

Use the direct console in the following cases:

- You are not satisfied with the IP address assigned by the DHCP server.
- You are not allowed to use the IP address assigned by the DHCP server.
- ESXi does not have an IP address. This situation could happen if the autoconfiguration phase did not succeed in configuring DHCP.
- The wrong network adapter was selected during the autoconfiguration phase.

Choose Network Adapters for the Management Network

Traffic between an ESXi host and any external management software is transmitted through an Ethernet network adapter on the host. You can use the direct console to choose the network adapters that are used by the management network.

Examples of external management software include the vSphere Client, vCenter Server, and SNMP client. Network adapters on the host are named vmnic*N*, where N is a unique number identifying the network adapter, for example, vmnic0, vmnic1, and so forth.

During the autoconfiguration phase, the ESXi host chooses vmnic0 for management traffic. You can override the default choice by manually choosing the network adapter that carries management traffic for the host. In some cases, you might want to use a Gigabit Ethernet network adapter for your management traffic. Another way to help ensure availability is to select multiple network adapters. Using multiple network adapters enables load balancing and failover capabilities.

Procedure

1 From the direct console, select **Configure Management Network** and press Enter.

2 Select **Network Adapters** and press Enter.

3 Select a network adapter and press Enter.

After the network is functional, you can use the vSphere Client to connect to the ESXi host.

Set the VLAN ID

You can set the virtual LAN (VLAN) ID number of the ESXi host.

Procedure

1 From the direct console, select **Configure Management Network** and press Enter.

2 Select **VLAN** and press Enter.

3 Enter a VLAN ID number from 1 through 4094.

Configuring IP Settings for ESXi

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

For future reference, write down the IP address.

For DHCP to work, your network environment must have a DHCP server. If DHCP is not available, the host assigns the link local IP address, which is in the subnet 169.254.x.x/16. The assigned IP address appears on the direct console. If you do not have physical monitor access to the host, you can access the direct console using a remote management application. See "Using Remote Management Applications," on page 27

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

Configure IP Settings from the Direct Console

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

Procedure

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

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

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

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

Configure IP Settings from the vSphere Client

If you do not have physical access to the host, you can use the vSphere Client to configure static IP settings if you are on the same physical subnet and you configure the vSphere Client IP to be on the 169.254.x.x network.

Procedure

1 Select the host in the inventory.

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

3 Click **Properties** next to Virtual Switch: vSwitch0.

4 Select **Management Network** and click **Edit**.

5 On the **IP Settings** tab, click **Use the following IP settings**.

6 Enter a static IP address, subnet mask, and default gateway and click **OK**.

Configure IP Settings from the vSphere Web Client

If you do not have physical access to the host, you can use the vSphere Web Client to configure static IP settings.

Procedure

1 Log in to the vCenter Server from the vSphere Web Client.

2 Select the host in the inventory.

3 On the **Manage** tab, select **Networking**.

4 Select **Virtual adapters**.

5 Select **vmk0 Management Network** and click the edit icon.

6 Select **IPv4 settings**.

7 Select **Use static IPv4 settings**.

8 Enter or change the static IPv4 address settings.

9 (Optional) Set static IPv6 addresses.

   a Select **IPv6 settings**.

   b Select **Static IPv6 addresses**.

   c Click the add icon.

   d Type the IPv6 address and click **OK**.

10 Click **OK**.

Configuring DNS for ESXi

You can select either manual or automatic DNS configuration of the ESXi host.

The default is automatic. For automatic DNS to work, your network environment must have a DHCP server and a DNS server.

In network environments where automatic DNS is not available or not desirable, you can configure static DNS information, including a host name, a primary name server, a secondary name server, and DNS suffixes.

Configure DNS Settings from the Direct Console

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

Procedure

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

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

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

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

Configure DNS Suffixes

If you have physical access to the host, you can use the direct console to configure DNS information. By default, DHCP acquires the DNS suffixes.

Procedure

1 From the direct console, select **Configure Management Network**.

2 Select **Custom DNS Suffixes** and press Enter.

3 Enter new DNS suffixes.

Test the Management Network

You can use the direct console to do simple network connectivity tests.

The direct console performs the following tests.

- Pings the default gateway
- Pings the primary DNS name server
- Pings the secondary DNS nameserver
- Resolves the configured host name

Procedure

1 From the direct console, select **Test Management Network** and press Enter.

2 Press Enter to start the test.

Restart the Management Agents

The management agents synchronize VMware components and let you access the ESXi host through the vSphere Client or vCenter Server. They are installed with the vSphere software. You might need to restart the management agents if remote access is interrupted.

Restarting the management agents restarts all management agents and services that are installed and running in `/etc/init.d` on the ESXi host. Typically, these agents include hostd, ntpd, sfcbd, slpd, wsman, and vobd. The software also restarts Fault Domain Manager (FDM) if it is installed.

Users accessing this host through the vSphere Client or vCenter Server lose connectivity when you restart management agents.

Procedure

1 From the direct console, select **Troubleshooting Options** and press Enter.

2 Select **Restart Management Agents** and press Enter.

3 Press F11 to confirm the restart.

The ESXi host restarts the management agents and services.

Restart the Management Network

Restarting the management network interface might be required to restore networking or to renew a DHCP lease.

Restarting the management network will result in a brief network outage that might temporarily affect running virtual machines.

If a renewed DHCP lease results in a new network identity (IP address or host name), remote management software will be disconnected.

Procedure

1 From the direct console, select **Restart Management Network** and press Enter.

2 Press F11 to confirm the restart.

Disable the Management Network

The management network synchronizes VMware components and lets you access the ESXi host through the vSphere Client or vCenter Server. It is installed with the vSphere software. You might need to disable the management network to isolate a host from the vCenter Server inventory.

Users who access this host through the vSphere Client or vCenter Server lose connectivity when you disable the management network.

One reason to disable the management network is to isolate an ESXi host from an HA and DRS cluster, without losing your static IP and DNS configurations or rebooting the host.

This operation does not require downtime for virtual machines. The virtual machines continue to run while the host is disconnected from vCenter Server and the vSphere Client.

Procedure

1 From the direct console, select **Disable Management Network** and press Enter.

2 Press F11 to confirm.

Restoring the Standard Switch

A vSphere Distributed Switch functions as a single virtual switch across all associated hosts. Virtual machines can maintain a consistent network configuration as they migrate across multiple hosts. If you migrate an existing standard switch, or virtual adapter, to a Distributed Switch and the Distributed Switch becomes unnecessary or stops functioning, you can restore the standard switch to ensure that the host remains accessible.

When you restore the standard switch, a new virtual adapter is created and the management network uplink that is currently connected to Distributed Switch is migrated to the new virtual switch.

You might need to restore the standard switch for the following reasons:

- The Distributed Switch is not needed or is not functioning.
- The Distributed Switch needs to be repaired to restore connectivity to vCenter Server and the hosts need to remain accessible.
- You do not want vCenter Server to manage the host. When the host is not connected to vCenter Server, most Distributed Switch features are unavailable to the host.

Prerequisites

Verify that your management network is connected to a distributed switch.

Procedure

1 From the direct console, select **Restore Standard Switch** and press Enter.

If the host is on a standard switch, this selection is dimmed, and you cannot select it.

2 Press F11 to confirm.

Test Connectivity to Devices and Networks

You can use the direct console to perform some simple network connectivity tests. In addition to the management network, you can specify other devices and networks.

Procedure

1 From the direct console, select **Test Management Network** and press Enter.

2 Type addresses to ping or another DNS host name to resolve.

3 Press Enter to start the test.

Storage Behavior

When you start ESXi, the host enters an autoconfiguration phase during which system storage devices are configured with defaults.

NOTE Partitioning for hosts that are upgraded to ESXi 5.x from ESXi versions earlier than version 5.0 differs significantly from partitioning for new installations of ESXi 5.x. See the *vSphere Upgrade* documentation.

When you reboot the ESXi host after installing the ESXi image, the host configures the system storage devices with default settings. By default, all visible blank internal disks are formatted with VMFS, so you can store virtual machines on the disks. In ESXi Embedded, all visible blank internal disks with VMFS are also formatted by default.

CAUTION ESXi overwrites any disks that appear to be blank. Disks are considered to be blank if they do not have a valid partition table or partitions. If you are using software that uses such disks, in particular if you are using logical volume manager (LVM) instead of, or in addition to, conventional partitioning schemes, ESXi might cause local LVM to be reformatted. Back up your system data before you power on ESXi for the first time.

On the hard drive or USB device that the ESXi host is booting from, the disk-formatting software retains existing diagnostic partitions that the hardware vendor creates. In the remaining space, the software creates the partitions described in Table 7-3.

Table 7-3. Partitions Created by ESXi on the Host Drive

ESXi Version	Partitions Created
ESXi Installable	For fresh installations, several new partitions are created for the boot banks, the scratch partition, and the locker. Fresh ESXi installations use GUID Partition Tables (GPT) instead of MSDOS-based partitioning. The partition table itself 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. One 4GB VFAT scratch partition is created for system swap. See "About the Scratch Partition," on page 181. The VFAT scratch partition is created only on the disk from which the ESXi host is booting. NOTE To create the VMFS volume and a scratch partition with the installation, the ESXi installer requires a minimum of 5.2GB of free space on the installation disk. The installer affects only the installation disk. The installer does not affect other disks of the server. When you install on a disk, the installer overwrites the entire disk. When the installer autoconfigures storage, the installer does not overwrite hardware vendor partitions. During ESXi installation, the installer creates a 110MB diagnostic partition for core dumps.
ESXi Embedded	One 110MB diagnostic partition for core dumps, if this partition is not present on another disk. The VFAT scratch and diagnostic partitions are created only on the disk from which the ESXi host is booting. On other disks, the software creates one VMFS5 partition per blank disk, using the whole disk. Only blank disks are formatted.
Both ESXi Installable and ESXi Embedded	One VMFS5 partition on the remaining free space.

You might want to override this default behavior if, for example, you use shared storage devices instead of local storage. To prevent automatic disk formatting, detach the local storage devices from the host under the following circumstances:

- Before you start the host for the first time.
- Before you start the host after you reset the host to the configuration defaults.

To override the VMFS formatting if automatic disk formatting already occurred, you can remove the datastore. See the *vCenter Server and Host Management* documentation.

About the Scratch Partition

For new installations of ESXi, during the autoconfiguration phase, a 4GB VFAT scratch partition is created if the partition is not present on another disk.

NOTE Partitioning for hosts that are upgraded to ESXi 5.x from ESXi versions earlier than version 5.0 differs significantly from partitioning for new installations of ESXi 5.x. See the *vSphere Upgrade* documentation.

When ESXi boots, the system tries to find a suitable partition on a local disk to create a scratch partition.

The scratch partition is not required. It is used to store vm-support output, which you need when you create a support bundle. If the scratch partition is not present, vm-support output is stored in a ramdisk. In low-memory situations, you might want to create a scratch partition if one is not present.

For the installable version of ESXi, the partition is created during installation and is selected. VMware recommends that you do not modify the partition.

NOTE To create the VMFS volume and scratch partition, the ESXi installer requires a minimum of 5.2GB of free space on the installation disk.

For ESXi Embedded, if a partition is not found, but an empty local disk exists, the system formats it and creates a scratch partition. If no scratch partition is created, you can configure one, but a scratch partition is not required. You can also override the default configuration. You might want to create the scratch partition on a remote NFS mounted directory.

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 simply lie idle.

Set the Scratch Partition from the vSphere Client

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

Prerequisites

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

Procedure

1. Use the vSphere Client to connect to the host.
2. Select the host in the Inventory.
3. In the **Configuration** tab, select **Software**.
4. Select **Advanced Settings**.
5. Select **ScratchConfig**.

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

Host Stops Unexpectedly at Bootup When Sharing a Boot Disk with Another Host

When more than one host, either physical or virtual, boots from the same shared physical disk or LUN, they cannot use the same scratch partition.

Problem

The host stops at bootup when sharing a boot disk with another host.

Cause

More than one ESXi host can share the same physical disk or LUN. When two such hosts also have the same scratch partition configured, either of the hosts can fail at bootup.

Solution

1 Set the hosts to boot sequentially, and boot the hosts.

   This setting lets you start the hosts so that you can change the scratch partition for one of them.

2 Use the vSphere Client to connect to one of the hosts.

3 Select the host in the Inventory.

4 In the **Configuration** tab, select **Software**.

5 Select **Advanced Settings**.

6 Select **ScratchConfig**.

   The field **ScratchConfig.CurrentScratchLocation** shows the current location of the scratch partition.

7 In the field **ScratchConfig.ConfiguredScratchLocation**, enter a directory path that is unique for this host.

8 Reboot the host for the changes to take effect.

View System Logs

System logs provide detailed information about system operational events.

Procedure

1 From the direct console, select **View System Logs**.

2 Press a corresponding number key to view a log.

   vCenter Server Agent (vpxa) logs appear if you add the host to vCenter Server.

3 Press Enter or the spacebar to scroll through the messages.

4 Perform a regular expression search.

   a Press the slash key (/).

   b Type the text to find.

   c Press Enter.

   The found text is highlighted on the screen.

5 Press q to return to the direct console.

What to do next

See also "Configure Syslog on ESXi Hosts," on page 183.

Configure Syslog on ESXi Hosts

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

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

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

Procedure

1 In the vSphere Client inventory, select the host.

2 Click the **Configuration** tab.

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

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

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

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified as [*datastorename*] *path_to_file* where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

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

   a Click **loggers**.

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

7 Click **OK**.

Changes to the syslog options take effect immediately.

Enable Lockdown Mode Using the Direct Console

To increase the security of your ESXi hosts, you can put them in lockdown mode.

When you enable lockdown mode, no users other than `vpxuser` have authentication permissions, nor can they perform operations against the host directly. Lockdown mode forces all operations to be performed through vCenter Server.

When a host is in lockdown mode, you cannot run vSphere CLI commands from an administration server, from a script, or from vMA against the host. External software or management tools might not be able to retrieve or modify information from the ESXi host.

NOTE Users with the DCUI Access privilege are authorized to log in to the Direct Console User Interface (DCUI) when lockdown mode is enabled. When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host. You grant the DCUI Access privilege in Advanced Settings.

Enabling or disabling lockdown mode affects which types of users are authorized to access host services, but it does not affect the availability of those services. In other words, if the ESXi Shell, SSH, or Direct Console User Interface (DCUI) services are enabled, they will continue to run whether or not the host is in lockdown mode.

You can enable lockdown mode using the Add Host wizard to add a host to vCenter Server, using the vSphere Client to manage a host, or using the direct console user interface.

NOTE If you enable or disable lockdown mode using the Direct Console User Interface (DCUI), permissions for users and groups on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using the vSphere Client connected to vCenter Server.

Lockdown mode is available only on ESXi hosts that you add to vCenter Server.

See the *vSphere Security* documentation for more information about lockdown mode.

Procedure

1 In the direct console, select **Configure Lockdown Mode** and press Enter.

2 Press the spacebar to select **Enable Lockdown Mode** and press Enter.

3 Press Enter.

The host is in lockdown mode.

Enable Lockdown Mode Using the vSphere Client

Enable lockdown mode to require that all configuration changes go through vCenter Server. You can also enable or disable lockdown mode through the Direct Console User Interface (DCUI).

Procedure

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

2 Select the host in the inventory panel.

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

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

The Lockdown Mode dialog box appears.

5 Select **Enable Lockdown Mode**.

6 Click **OK**.

Enable Lockdown Mode Using the vSphere Web Client

Enable lockdown mode to require that all configuration changes go through vCenter Server. You can also enable or disable lockdown mode through the Direct Console User Interface (DCUI).

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Security Profile**.

4 In the Lockdown Mode panel, click **Edit**.

5 Select **Enable Lockdown Mode**.

6 Click **OK**.

Enable ESXi Shell and SSH Access with the Direct Console User Interface

Use the direct console user interface to enable the ESXi Shell.

Procedure

1 From the Direct Console User Interface, press F2 to access the System Customization menu.

2 Select **Troubleshooting Options** and press Enter.

3 From the Troubleshooting Mode Options menu, select a service to enable.

- Enable ESXi Shell
- Enable SSH

4 Press Enter to enable the service.

5 (Optional) Set the timeout for the ESXi Shell.

By default, timeouts for the ESXi Shell is 0 (disabled).

The availability timeout setting is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, if you have not logged in, the shell is disabled.

NOTE If you are logged in when the timeout period elapses, your session will persist. However, the ESXi Shell will be disabled, preventing other users from logging in.

a From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.

b Enter the availability timeout in minutes.

The availability timeout is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled.

c Press Enter.

d Enter the idle timeout.

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

6 Press Esc until you return to the main menu of the Direct Console User Interface.

Set the Host Image Profile Acceptance Level

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

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

See "Acceptance Levels," on page 149.

Prerequisites

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

Procedure

1 Use the vSphere Client to access the host in one of the following ways.

- Connect to the host directly.
- Connect to vCenter Server, and select the host in the inventory.

2 Click the **Configuration** tab.

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

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

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

Table 7-4. Host Image Profile Acceptance Levels

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMwareCertified	VMwareCertified
VMwareAccepted	VMwareCertified, VMwareAccepted
PartnerSupported	VMwareCertified, VMwareAccepted, PartnerSupported
CommunitySupported	VMwareCertified, VMwareAccepted, PartnerSupported, CommunitySupported

Reset the System Configuration

If you are having trouble determining the source of a problem with your ESXi host, you can reset the system configuration.

Changes in the system configuration can be related to various problems, including problems with connectivity to the network and devices. Resetting the system configuration might solve such problems. If resetting the system configuration does not solve the problem, it can still rule out configuration changes made since the initial setup as the source of the problem.

When you reset the configuration, the software overrides all your configuration changes, deletes the password for the administrator account (root), and reboots the host. Configuration changes made by your hardware vendor, such as IP address settings and license configuration, might also be deleted.

Resetting the configuration does not remove virtual machines on the ESXi host. After you reset the configuration defaults, the virtual machines are not visible, but you make them visible again by reconfiguring storage and reregistering the virtual machines.

CAUTION When you reset the configuration defaults, users accessing the host lose connectivity.

Prerequisites

Before resetting the configuration, back up your ESXi configuration in case you want to restore your configuration.

Procedure

1 Back up the configuration using the vSphere CLI `vicfg-cfgbackup` command.

2 From the direct console, select **Reset System Configuration** and press Enter.

3 Press F11 to confirm.

The system reboots after all settings are reset to the default values.

Remove All Custom Packages on ESXi

After adding custom packages, you might decide to remove them.

Prerequisites

Before you remove custom packages, shut down or migrate running virtual machines off of the ESXi host.

Procedure

1 Reboot the ESXi host.

2 In the direct console, select **Remove Custom Extensions** and press F11 to confirm.

3 Reboot the host.

All custom packages are removed.

Disable Support for Non-ASCII Characters in Virtual Machine File and Directory Names

By default, ESXi supports the use of non-ASCII characters for virtual machine file and directory names. You can disable this support by modifying the `/etc/vmware/hostd/config.xml` file.

After you disable this support, you can still enter non-ASCII characters for virtual machine names. vSphere user interfaces will display the virtual machine names in the non-ASCII characters, but ESXi will convert the actual file and directory names to ASCII strings.

Procedure

1 Using a text editor, open the `/etc/vmware/hostd/config.xml` file for the ESXi host.

2 Within the `<config></config>` tag, add the following code.

```
<g11nSupport>false</g11nSupport>
```

3 Save and close the file.

4 Reboot the host.

Disable ESXi

If you do not want your server to be an ESXi host, you can deactivate the ESXi setup.

Procedure

1 Remove VMFS datastores on the internal disks so that the internal disks are no longer set up to store virtual machines.

2 Change the boot setting in the BIOS so that the host no longer boots into ESXi.

3 Install another operating system in its place.

8 After You Install and Set Up ESXi

After ESXi is installed and set up, consider managing the host through the vSphere Client, licensing the host, and backing up your ESXi configuration.

This chapter includes the following topics:

Managing the ESXi Host with the vSphere Client and the vSphere Web Client

The vSphere Client and the vSphere Web Client provide simplest way to manage your ESXi host and operate its virtual machines.

You can use the vSphere Client to connect directly to the ESXi host. If you use vCenter Server, you can also use the vSphere Client to connect to and operate vCenter Server. You can use the vSphere Web Client to connect to and operate vCenter Server by Web browser.

To install the vSphere Client and the vSphere Web Client, see the following topics

- vSphere Client
  - "Download the vSphere Client," on page 280
  - "Install the vSphere Client," on page 280
  - "Start the vSphere Client," on page 281
- vSphere Web Client
  - "Install or Upgrade the vSphere Web Client," on page 282

Licensing ESXi Hosts

vSphere provides several ways to license your hosts.

You can use vCenter Server or the vSphere Client to license an individual host.

For information about managing host licenses, see *Managing Licenses on ESXi Hosts* in *vCenter Server and Host Management*.

You can set up bulk licensing using PowerCLI commands. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with Auto Deploy. See "Set Up Bulk Licensing," on page 80.

You can also operate ESXi without licensing for a 60-day evaluation period, during which you can access the full ESXi feature set. See "About ESXi Evaluation and Licensed Modes," on page 16

About ESXi Evaluation and Licensed Modes

After you purchase vSphere licenses, VMware provides a serial number that you use to license ESXi hosts. You can use evaluation mode to explore the entire set of features that are available for ESXi hosts, including features that are not included in the license that you have.

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.

For information about managing licensing and setting an ESXi host to evaluation mode, see the *vCenter Server and Host Management* documentation.

Recording the ESXi License Key

All ESXi editions have license keys associated with them. VMware recommends that you write down the license key and tape it to the server, or put the license key in a secure, easily accessible location.

You can access the license key from the direct console or the vSphere Client. If the host becomes inaccessible or unbootable, it is important that you have a record of the license key.

Access the ESXi License Key from the Direct Console

If you have physical access to the host or remote access to the direct console, you can use the direct console to access the ESXi license key.

Procedure

- From the direct console, select **View Support Information**.

  The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, labeled License Serial Number.

  NOTE The physical machine serial number also appears, labeled Serial Number. Do not confuse the license key with the physical machine serial number.

Access the ESXi License Key from the vSphere Client

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

Procedure

1. From the vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab and click **Licensed Features**.

   The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Access the ESXi License Key from the vSphere Web Client

You can use the vSphere Web Client to access the ESXi license key.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Select the **Manage** tab.

4 Select **Settings**.

5 Select **System**.

6 Select **Licensing**.

The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Preparing vCenter Server Databases 9

vCenter Server and vSphere Update Manager require databases to store and organize server data.

Each vCenter Server instance must have its own database. vCenter Server instances cannot share the same database schema. Multiple vCenter Server databases can reside on the same database server, or they can be separated across multiple database servers. For Oracle databases, which have the concept of schema objects, you can run multiple vCenter Server instances in a single database server if you have a different schema owner for each vCenter Server instance. You can also use a dedicated Oracle database server for each vCenter Server instance.

You do not need to install a new database server for the vCenter Server installation to work. During vCenter Server installation, you can point the vCenter Server system to any existing supported database. vCenter Server supports IBM DB2, Oracle, and Microsoft SQL Server databases. Update Manager supports Oracle and Microsoft SQL Server databases. For information about supported database server versions, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Caution If you have a VirtualCenter database that you want to preserve, do not perform a fresh installation of vCenter Server. See the *vSphere Upgrade* documentation.

VMware recommends using separate databases for vCenter Server and Update Manager. For a small deployments, a separate database for Update Manager might not be necessary.

This chapter includes the following topics:

vCenter Server Database Configuration Notes

After you choose a supported database type, make sure you understand any special configuration requirements.

Table 9-1 is not a complete list of databases supported with vCenter Server. For information about specific database versions and service pack configurations supported with vCenter Server, see the VMware Product Interoperability Matrixes. This topic is intended only to provide special database configuration notes not listed in the Product Interoperability Matrixes.

vCenter Server databases require a UTF code set.

Contact your DBA for the appropriate database credentials.

Table 9-1. 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. 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. If Microsoft SQL Server 2005 is not already installed and the machine has MSXML Core Services 6.0 installed, remove MSXML Core Services 6.0 before installing Microsoft SQL Server 2005. If you cannot remove it using the Add or Remove Programs utility, use the Windows Installer CleanUp utility. See http://support.microsoft.com/kb/968749. NOTE This database is not supported for the vCenter Server Appliance.
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	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.

Create a 64-Bit DSN

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

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.

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.

About the Bundled Microsoft SQL Server 2008 R2 Express Database Package

The bundled Microsoft SQL Server 2008 R2 Express database package is installed and configured when you select the bundled database during vCenter Server installation or upgrade.

To install the bundled Microsoft SQL Server 2008 R2 Express database, 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.

Maintaining a vCenter Server Database

After your vCenter Server database instance and vCenter Server are installed and operational, perform standard database maintenance processes.

The standard database maintenance processes include the following:

- Monitoring the growth of the log file and compacting the database log file, as needed.
- Scheduling regular backups of the database.
- Backing up the database before any vCenter Server upgrade.

See your database vendor's documentation for specific maintenance procedures and support.

Configure DB2 Databases

If you use a DB2 database for your vCenter Server repository, you need to configure your database to work with vCenter Server.

Procedure

1 Configure an IBM DB2 Database User and Group on page 197

To use an IBM DB2 database when you install vCenter Server, you must configure the database user and group.

2 Add the Database Instance Registry Variables on page 197

After connecting to the server as DB2 instance owner, you can configure the DB2 registry variables on the database server.

3 Add the Client Instance Registry Variable on page 198

After connecting to the server as DB2 instance owner, you can configure the DB2 registry variables on the vCenter Server.

4 Use a Script to Create a DB2 Database on page 199

When you use a DB2 database with vCenter Server, the database must have certain buffer pools, table spaces, and privileges. To simplify the process of creating the database, you can run a DB2 script.

5 (Optional) Use a Script to Create the DB2 Database Schema on page 200

The vCenter Server installer creates the schema during installation. Experienced database administrators who need more control over schema creation because of environmental constraints can use a script to create their database schema.

6 Configure a Connection to a Local DB2 Database on Microsoft Windows on page 202

You can configure a DB2 database for vCenter Server locally on the same Microsoft Windows machine as vCenter Server.

7 Prepare to Configure a Connection to a Remote DB2 Database on page 203

Configuring a connection to a remote DB2 database on Linux, UNIX, or Microsoft Windows requires several preparatory steps..

8 Configure a Connection to a Remote DB2 Database on Linux, UNIX, or Microsoft Windows on page 203

You can configure a DB2 database for vCenter Server remotely on a network-connected Microsoft Windows, Linux, or UNIX host.

9 (Optional) Configure an IBM DB2 Database User to Enable Database Monitoring on page 204

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime due to a lack of resources for the database server.

Configure an IBM DB2 Database User and Group

To use an IBM DB2 database when you install vCenter Server, you must configure the database user and group.

You can configure a DB2 database for vCenter Server either locally on the same Microsoft Windows machine as vCenter Server or remotely on a network-connected Linux, UNIX, or Windows host.

Prerequisites

- Review the software requirements for vCenter Server with DB2.
- Verify that a DB2 instance is created and configured for incoming TCP connections. See the DB2 documentation Web site.
- Make sure that you created a user called vcx.
- The DB2 database server must use codeset UTF-8.

Procedure

1 Create an initial user on the operating system.

By default, DB2 uses the operating system authentication for all its database users.

2 If the database is hosted on a Microsoft Windows machine, add the user vcx as a member of the group DB2USERS.

3 Create a user group called DBSYSMON and add the user vcx as a member.

4 Open a DB2 command window or Command Line Processor (CLP) as the DB2 instance owner.

- On Microsoft Windows, select **Start > IBM DB2 > DB2Copy1 > Command Line Tools > Command Window**.
- On Linux or UNIX, open a terminal and switch your user to the DB2 instance owner.

5 In the DB2 command window, run the following commands to add the appropriate user group to the group of users capable of database system monitoring:

```
db2 update dbm cfg using sysmon_group dbsysmon
```

This command affects all databases in this instance.

You now have a DB2 database user that you can reference in the vCenter Server installer.

What to do next

Add the database instance registry variables.

Add the Database Instance Registry Variables

After connecting to the server as DB2 instance owner, you can configure the DB2 registry variables on the database server.

Prerequisites

Make sure that you configure an IBM DB2 database user and group.

Procedure

1 Open a DB2 Command window or Command Line Processor (CLP) as the DB2 instance owner.

- On Microsoft Windows, select **Start > IBM DB2 > DB2Copy1 > Command Line Tools > Command Window**.
- On Linux or UNIX, open a terminal and switch your user to the DB2 instance owner.

2 Start the DB2 instance.

```
db2start
```

3 Enable the DB2 administrative task scheduler.

```
db2set DB2_ATS_ENABLE=YES
```

4 Enable the DB2 database system to ignore uncommitted insertions.

```
db2set DB2_SKIPINSERTED=ON
```

5 Enable the table or index access scans to defer or avoid row locking until a data record is known to satisfy predicate evaluation.

```
db2set DB2_EVALUNCOMMITTED=ON
```

6 Enable the DB2 database system to skip deleted keys during index access and skip deleted rows during table access.

```
db2set DB2_SKIPDELETED=ON
```

7 Stop and restart the database instance.

```
db2stop force
db2start
```

These commands affect all databases in this instance.

All the required registry variables are set up.

What to do next

Add the client instance registry variable.

Add the Client Instance Registry Variable

After connecting to the server as DB2 instance owner, you can configure the DB2 registry variables on the vCenter Server.

Prerequisites

- Configure an IBM DB2 database user and group.
- Add the database instance registry variables.
- Make sure that the DB2 runtime client is installed on the Windows machine that will host vCenter Server. If the database server and the vCenter Server are running on the same machine, you do not have to install the runtime client separately.

Procedure

1 Open a DB2 Command window or Command Line Processor (CLP) as the DB2 instance owner.

- On Microsoft Windows, select **Start > IBM DB2 > DB2Copy1 > Command Line Tools > Command Window**.
- On Linux or UNIX, open a terminal and switch your user to the DB2 instance owner.

2 To configure the vSphere Client to behave as a Unicode application, set the DB2CODEPAGE registry variable to 1208.

```
db2set DB2CODEPAGE=1208
```

NOTE If you are configuring the DB2 database on the same machine as the one that is running vCenter Server, you need to run the db2set command after connecting to the database server (which is the same as the vCenter Server host).

What to do next

Create the DB2 database, including all necessary buffer pools, table spaces, and privileges.

Use a Script to Create a DB2 Database

When you use a DB2 database with vCenter Server, the database must have certain buffer pools, table spaces, and privileges. To simplify the process of creating the database, you can run a DB2 script.

Prerequisites

- Configure an IBM DB2 database user and group.
- Add the database instance registry variables.
- Add the client instance registry variable.

Procedure

1 Copy the following DB2 script into a text editor and save it with a descriptive filename, such as vcdbcreate.sql.

The script is located in the */installation directory*/vpx/dbschema/db2_prereq_connection_configuration.txt vCenter Server installation package file.

```
CREATE DATABASE VCDB
AUTOMATIC STORAGE YES ON 'C:\'
DBPATH ON 'C:\' USING CODESET UTF-8
TERRITORY US
COLLATE USING SYSTEM PAGESIZE 4096;

UPDATE DB CFG FOR VCDB USING AUTO_MAINT ON;
UPDATE DB CFG FOR VCDB USING AUTO_TBL_MAINT ON;
UPDATE DB CFG FOR VCDB USING AUTO_RUNSTATS ON;
UPDATE DB CFG FOR VCDB USING logprimary 32 logsecond 6 logfilsiz 2048;
UPDATE ALERT CFG FOR DATABASE ON VCDB USING db.db_backup_req SET THRESHOLDSCHECKED YES;
UPDATE ALERT CFG FOR DATABASE ON VCDB USING db.tb_reorg_req SET THRESHOLDSCHECKED YES;
UPDATE ALERT CFG FOR DATABASE ON VCDB USING db.tb_runstats_req SET THRESHOLDSCHECKED YES;

CONNECT TO VCDB;
CREATE BUFFERPOOL VCBP_8K IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 8K;
CREATE LARGE TABLESPACE VCTS_8k PAGESIZE 8K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 32
OVERHEAD 12.67 PREFETCHSIZE 32 TRANSFERRATE 0.18 BUFFERPOOL VCBP_8K;
CREATE BUFFERPOOL VCBP_16K IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 16K;
CREATE LARGE TABLESPACE VCTS_16k PAGESIZE 16K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 32
OVERHEAD 12.67 PREFETCHSIZE 32 TRANSFERRATE 0.18 BUFFERPOOL VCBP_16K;
CREATE BUFFERPOOL VCBP_32K IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 32K;
CREATE LARGE TABLESPACE VCTS_32k PAGESIZE 32K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 32
OVERHEAD 12.67 PREFETCHSIZE 32 TRANSFERRATE 0.18 BUFFERPOOL VCBP_32K;
CREATE TABLESPACE SYSTOOLSPACE IN IBMCATGROUP MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 4;
```

```
CREATE USER TEMPORARY TABLESPACE SYSTOOLSTMPSPACE IN IBMCATGROUP MANAGED BY AUTOMATIC STORAGE
EXTENTSIZE 4;
CREATE SYSTEM TEMPORARY TABLESPACE VCTEMPTS_8K PAGESIZE 8K MANAGED BY AUTOMATIC STORAGE
BUFFERPOOL VCBP_8K;
CREATE SYSTEM TEMPORARY TABLESPACE VCTEMPTS_16K PAGESIZE 16K MANAGED BY AUTOMATIC STORAGE
BUFFERPOOL VCBP_16K;
CREATE SYSTEM TEMPORARY TABLESPACE VCTEMPTS_32K PAGESIZE 32K MANAGED BY AUTOMATIC STORAGE
BUFFERPOOL VCBP_32K;

GRANT USE OF TABLESPACE VCTS_16K TO USER vcx WITH GRANT OPTION;
GRANT USE OF TABLESPACE VCTS_32K TO USER vcx WITH GRANT OPTION;
GRANT USE OF TABLESPACE VCTS_8K TO USER vcx WITH GRANT OPTION;

commit work;
connect reset;
terminate;
```

2 Customize the following values in the script.

- Database name: VCDB. You must use the same value for the ODBC setup.
- Database path: `C:\` for Microsoft Windows, or a UNIX path with sufficient permissions.
- User name: vcx. You must use the same value for the ODBC setup.

Do not modify the script in any other way. Changing the setup for table spaces or buffer pools might prevent successful installation of vCenter Server.

3 Run the script in a DB2 Command window.

```
db2 –svtf vcdbcreate.sql
```

You now have a DB2 database that you can use with vCenter Server.

What to do next

Configure a connection to a local or remote database.

(Optional) Use a Script to Create the DB2 Database Schema

The vCenter Server installer creates the schema during installation. Experienced database administrators who need more control over schema creation because of environmental constraints can use a script to create their database schema.

To have the vCenter Server installer create your schema for you, see "Configure a Connection to a Local DB2 Database on Microsoft Windows," on page 202 or "Configure a Connection to a Remote DB2 Database on Linux, UNIX, or Microsoft Windows," on page 203, depending on your environment.

Prerequisites

Create the DB2 database and user. You can create the DB2 database manually or by using scripts.

Procedure

1 Open a DB2 Command Editor window and log in as the user that you created on the vCenter Server database.

a Open DB2 Control Center.

b Select the database.

c Right-click the database and select **Menu > Query**.

2 In the directory of the vCenter Server installation package */installation directory*/vpx/dbschema, locate the dbschema scripts.

3 In the DB2 Command Editor window, open the SQL files one at a time and press Ctrl+Enter to run each SQL file query in the order shown here.

```
VCDB_db2.sql
TopN_DB_db2.sql
```

For the following files, change the statement termination character from ; to @.

```
load_stats_proc_db2.sql
purge_stat2_proc_db2.sql
purge_stat3_proc_db2.sql
purge_usage_stats_proc_db2.sql
stats_rollup1_proc_db2.sql
stats_rollup2_proc_db2.sql
stats_rollup3_proc_db2.sql
cleanup_events_db2.sql
delete_stats_proc_db2.sql
upsert_last_event_proc_db2.sql
load_usage_stats_proc_db2.sql
calc_topn1_proc_db2.sql
calc_topn2_proc_db2.sql
calc_topn3_proc_db2.sql
calc_topn4_proc_db2.sql
clear_topn1_proc_db2.sql
clear_topn2_proc_db2.sql
clear_topn3_proc_db2.sql
clear_topn4_proc_db2.sql
rule_topn1_proc_db2.sql
rule_topn2_proc_db2.sql
rule_topn3_proc_db2.sql
rule_topn4_proc_db2.sql
process_license_snapshot_db2.sql
l_stats_rollup3_proc_db2.sql
l_purge_stat2_proc_db2.sql
l_purge_stat3_proc_db2.sql
l_stats_rollup1_proc_db2.sql
l_stats_rollup2_proc_db2.sql
process_temptable0_proc_db2.sql
process_temptable1_proc_db2.sql
process_temptable2_proc_db2.sql
job_schedule2_db2.sql
job_schedule3_db2.sql
job_cleanup_events_db2.sql
job_topn_past_day_db2.sql
job_topn_past_week_db2.sql
job_topn_past_month_db2.sql
job_topn_past_year_db2.sql
job_property_bulletin_db2
```

You now have a database schema that is compatible with vCenter Server.

4 (Optional) you can also run the following scripts to enable database health monitoring. Use @ for the statement termination character.

```
job_dbm_performance_data_db2.sql
process_performance_data_db2.sql
```

5 On the machine that you intend to install vCenter Server on, create a data source name (DSN) that points to the database server that has the schema.

6 Run the vCenter Server installer.

When prompted, provide the database user login.

7 If a database reinitialization warning message appears in the vCenter Server installer, select **Do not overwrite, leave my existing database in place** and continue the installation.

This message appears if you are using a database that has vCenter Server tables that were created by a previous installation. The message does not appear if the database is clean.

If you leave your existing database in place, you cannot join the vCenter Server to a Linked Mode group during the installation. You can join after the installation is complete. (See "Join a Linked Mode Group After Installation," on page 296.)

Configure a Connection to a Local DB2 Database on Microsoft Windows

You can configure a DB2 database for vCenter Server locally on the same Microsoft Windows machine as vCenter Server.

NOTE The vCenter Server installer should generate and validate the JDBC URL for the vCenter Server database. However, if you use a local, or indirect, DB2 database, the DB2 analyzer is not able to construct the JDBC URL. You can add the JDBC URL manually. See "JDBC URL Formats for the vCenter Server Database," on page 234.

Prerequisites

- Configure a user and group for the database.
- Add the database instance registry variables.
- Add the client instance registry variable.
- Create the database with the required buffer pools, table spaces, and privileges.

Procedure

1 On the Microsoft Windows machine that will host vCenter Server, click **Start > Run** to open the Microsoft ODBC Administrator utility.

2 Type **`odbcad32.exe`**.

3 On the **System DSN** tab, click **Add**.

4 Select the driver that corresponds to your database (for example, **IBM DB2 ODBC Driver - VCDB2Add**) and click **Finish**.

5 Enter a name for the DSN (for example, **`VCDB2`**), and select your database from the menu.

6 Select the DSN and click **Configure** to verify that the database connection works.

7 Type the database user name (for example, **`vcx`**) and password.

8 Click **Connect**.

The DB2 database is configured.

What to do next

Optionally, you can enable Database Monitoring for DB2 database users. Otherwise, install vCenter Server. When the vCenter Server installer prompts you for a DSN, point to the DSN that you created in this procedure.

Prepare to Configure a Connection to a Remote DB2 Database

Configuring a connection to a remote DB2 database on Linux, UNIX, or Microsoft Windows requires several preparatory steps..

Procedure

1 Download the IBM Data Server Driver for ODBC and CLI from the IBM Software Web site.

2 On the remote machine, take the following steps.

   a Configure a database user and group.

   b Create the database with the required buffer pools, table spaces, and privileges.

   c Add the database instance registry variables.

3 On the machine where vCenter Server will be installed, take the following steps.

   a Add the client instance registry variable.

   b Make sure that the IBM Data Server Runtime Client is installed

4 On the machine where vCenter Server will be installed, catalog the server node and the database.

   In a command window, run the following commands.

   ```
   db2 catalog tcpip node name remote DB Server host name or IP Address server Port number used

   db2 catalog db database name at node name authentication SERVER
   ```

Configure a Connection to a Remote DB2 Database on Linux, UNIX, or Microsoft Windows

You can configure a DB2 database for vCenter Server remotely on a network-connected Microsoft Windows, Linux, or UNIX host.

Prerequisites

See "Prepare to Configure a Connection to a Remote DB2 Database," on page 203.

Procedure

1 On the Microsoft Windows machine that will host vCenter Server, select **Start > Run**.

2 Type **odbcad32.exe** to open the Microsoft ODBC Administrator utility.

3 On the **System DSN** tab, click **Add**.

4 Select the driver that corresponds to your database (for example, IBM DB2 ODBC Driver - VCDB2_remote) and click **Finish**.

5 In the IBM DB2 Driver Add dialog box, configure the database values.

   - Database name. The default value is vcdb.
   - Database alias. The database alias can be the same as the database name.
   - DSN name. For example, VCDB2.

You have completed the DB2 database configuration.

What to do next

Optionally, you can enable Database Monitoring for DB2 database users. Otherwise, you can now install vCenter Server. When the vCenter Server installer prompts you for a DSN, point to the DSN that you created in this procedure.

(Optional) Configure an IBM DB2 Database User to Enable Database Monitoring

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime due to a lack of resources for the database server.

Database Monitoring for vCenter Server enables administrators to monitor the database server CPU, memory, I/O, data storage, and other environment factors for stress conditions. Statistics are stored in the vCenter Server Profile Logs.

Prerequisites

Configure the IBM DB2 database user group DBSYSMON, and add the group to the group of users capable of database system monitoring. See "Configure an IBM DB2 Database User and Group," on page 197.

Procedure

- Make sure the database user is a member of the DBSYSMON group.

  Database Monitoring is enabled for all members of the DBSYSMON group.

What to do next

Install vCenter Server.

Configure Microsoft SQL Server Databases

To use a Microsoft SQL database for your vCenter Server repository, configure your database to work with vCenter Server.

Procedure

1 Create a SQL Server Database and User for vCenter Server on page 205

   You must create a database and user for vCenter Server. To simplify the process, you can use a script.

2 Set Database Permissions By Manually Creating Database Roles and the VMW Schema on page 206

   By using this recommended method, available with vCenter Server 5.x, the vCenter Server database administrator can set permissions for vCenter Server users and administrators to be granted through Microsoft SQL Server database roles.

3 Set Database Permissions by Using the dbo Schema and the db_owner Database Role on page 207

   If you use Microsoft SQL Server database, the simplest way to assign permissions for a vCenter Server database user is through the database role **db_owner**. Assign the **db_owner** role to the vCenter Server database user on both the vCenter and MSDB databases.

4 Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role on page 207

   If you set database permissions by using the dbo schema and db_owner database role, you can use a script to create a vCenter Server user with the db_owner database role.

5 Use a Script to Create a Microsoft SQL Server Database Schema and Roles on page 208

   In this recommended method of configuring the SQL database, you create the custom schema VMW, instead of using the existing dbo schema.

6 (Optional) Use a Script to Create Microsoft SQL Server Database Objects Manually on page 209

You can create database objects manually with this method of configuring the SQL database.

7 Configure a SQL Server ODBC Connection on page 212

After you create a vCenter Server user, establish a connection with a SQL Server database. This connection is required to install a vCenter Server system.

8 Configure Microsoft SQL Server TCP/IP for JDBC on page 213

If the Microsoft SQL Server database has TCP/IP disabled and the dynamic ports are not set, the JDBC connection remains closed. The closed connection causes the vCenter Server statistics to malfunction. You can configure the server TCP/IP for JDBC.

9 (Optional) Configure a Microsoft SQL Server Database User to Enable Database Monitoring on page 214

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime because of a lack of resources for the database server.

Create a SQL Server Database and User for vCenter Server

You must create a database and user for vCenter Server. To simplify the process, you can use a script.

In the script, you can customize the location of the data and log files.

The user that is created by this script is not subject to any security policy. Change the passwords as appropriate.

Procedure

1 Log in to a Microsoft SQL Server Management Studio session as the sysadmin (SA) or a user account with **sysadmin** privileges.

2 Run the following script.

The script is located in the vCenter Server installation package at `/<installation directory>/vpx/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
use [master]
go
CREATE DATABASE [VCDB] ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\VCDB.mdf', SIZE = 2000KB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
sp_addlogin @loginame=[vpxuser], @passwd=N'vpxuser!0', @defdb='VCDB',
@deflanguage='us_english'
go
ALTER LOGIN [vpxuser] WITH CHECK_POLICY = OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use MSDB
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
```

You now have a Microsoft SQL Server database that you can use with vCenter Server.

What to do next

See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206.

Set Database Permissions By Manually Creating Database Roles and the VMW Schema

By using this recommended method, available with vCenter Server 5.x, the vCenter Server database administrator can set permissions for vCenter Server users and administrators to be granted through Microsoft SQL Server database roles.

VMware recommends this method because it removes the requirement to set up the database dbo schema and **db_owner** role for vCenter Server users who install and upgrade vCenter Server.

Alternatively, you can assign vCenter Server database permissions by creating and assigning the **db_owner** role and letting the vCenter Server installer create the default schema that assigns database user permissions to that role. See "Set Database Permissions by Using the dbo Schema and the db_owner Database Role," on page 207.

Prerequisites

Create the vCenter Server database. See "Create a SQL Server Database and User for vCenter Server," on page 205

Procedure

1. Create the database VCDB and the database schema VMW in VCDB.
2. Assign the default schema VMW to the user **[vpxuser]**.
3. In the vCenter Server database, create the user role **VC_ADMIN_ROLE**.
4. In the vCenter Server database, grant privileges to the **VC_ADMIN_ROLE**.
   a. Grant the schema permissions **ALTER**, **REFERENCES**, and **INSERT**.
   b. Grant the permissions **CREATE TABLE**, **VIEW**, and **CREATE PROCEDURES**.
5. In the vCenter Server database, create the **VC_USER_ROLE**.
6. In the vCenter Server database, grant the schema permissions **SELECT**, **INSERT**, **DELETE**, **UPDATE**, and **EXECUTE** to the **VC_USER_ROLE**.
7. Grant the **VC_USER_ROLE** to the user **[vpxuser]**.
8. Grant the **VC_ADMIN_ROLE** to the user **[vpxuser]**.
9. In the MSDB database, create the user **[vpxuser]**.
10. In the MSDB database, create the user role **VC_ADMIN_ROLE**.
11. Grant privileges to the **VC_ADMIN_ROLE** in MSDB.
    a. On the MSDB tables `syscategories`, `sysjobsteps`, and `sysjobs`, grant the **SELECT** permission to the user **[vpxuser]**.
    b. On the MSDB stored procedures `sp_add_job`, `sp_delete_job`, `sp_add_jobstep`, `sp_update_job`, `sp_add_jobserver`, `sp_add_jobschedule`, and `sp_add_category`, grant the **EXECUTE** permission to the role **VC_ADMIN_ROLE**.
12. In the MSDB database, grant the **VC_ADMIN_ROLE** to the user **[vpxuser]**.
13. Connect to the vCenter Server database as user **[vpxuser]** and create the ODBC DSN.
14. Install vCenter Server.
15. Revoke the **VC_ADMIN_ROLE** from the user **[vpxuser]** in vCenter Server database

The hardcoded **dbo** role is removed from `VCDB_mssql.sql`.

What to do next

"Use a Script to Create a Microsoft SQL Server Database Schema and Roles," on page 208

Set Database Permissions by Using the dbo Schema and the db_owner Database Role

If you use Microsoft SQL Server database, the simplest way to assign permissions for a vCenter Server database user is through the database role **db_owner**. Assign the **db_owner** role to the vCenter Server database user on both the vCenter and MSDB databases.

Alternatively, experienced database administrators can set permissions by creating database roles and the VMW schema manually. See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206 and "Use a Script to Create a Microsoft SQL Server Database Schema and Roles," on page 208. That method, available beginning with vSphere 5.0, is recommended, because it gives the database administrator greater control over database permissions. The recommended method also removes the requirement to set up the database dbo schema and **db_owner** role for vCenter Server users who install and upgrade vCenter Server.

Prerequisites

Create the vCenter Server database. See "Create a SQL Server Database and User for vCenter Server," on page 205

Procedure

1 Assign the role **dbo** to the vCenter Server and Microsoft SQL databases.

2 For any user who will install or upgrade vCenter Server, assign the user the default schema dbo.

When you install vCenter Server, the installer uses the default dbo schema to assign permissions to the **db_owner** role.

Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role

If you set database permissions by using the dbo schema and db_owner database role, you can use a script to create a vCenter Server user with the db_owner database role.

Alternatively, experienced database administrators can set permissions by creating database roles and the VMW and SQL Server database schemas. See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206"Use a Script to Create a Microsoft SQL Server Database Schema and Roles," on page 208. That method, available beginning with vSphere 5.0, is recommended, because it gives the database administrator greater control over database permissions. That method removes the requirement to set up the database role **dbo** and db_owner schema for vCenter Server users who install and upgrade vCenter Server.

Prerequisites

Create the vCenter Server database. See "Create a SQL Server Database and User for vCenter Server," on page 205

Procedure

1 Log in to a Microsoft SQL Server Management Studio session as the sysadmin (SA) or a user account with **sysadmin** privileges.

2 Run the following script.

The script is located in the vCenter Server installation package */installation directory*/vpx/dbschema/DB_and_schema_creation_scripts_MSSQL.txt file.

```
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
```

What to do next

"Configure a SQL Server ODBC Connection," on page 212

Use a Script to Create a Microsoft SQL Server Database Schema and Roles

In this recommended method of configuring the SQL database, you create the custom schema VMW, instead of using the existing dbo schema.

This method requires that you create new database roles and grant them to the database *user*. See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206 and "Use a Script to Create a Microsoft SQL Server Database Schema and Roles," on page 208.

Prerequisites

Create the SQL Server database and user for vCenter Server. You can create the database manually or by using a script. See "Create a SQL Server Database and User for vCenter Server," on page 205

Procedure

1 Log in to a Microsoft SQL Server Management Studio session as the sysadmin (SA) or a user account with sysadmin privileges.

2 Run the following script.

The script is located in the vCenter Server installation package at */installation directory*/vpx/dbschema/DB_and_schema_creation_scripts_MSSQL.txt

```
CREATE SCHEMA [VMW]
go
ALTER USER [vpxuser] WITH DEFAULT_SCHEMA =[VMW]
go

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA ::  [VMW] to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
```

```
GRANT SELECT ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT EXECUTE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , [vpxuser]
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
```

(Optional) Use a Script to Create Microsoft SQL Server Database Objects Manually

You can create database objects manually with this method of configuring the SQL database.

Alternatively, you can configure a SQL Server ODBC connection and run the Install package. The vCenter Server installer will create database objects. See"Configure a SQL Server ODBC Connection," on page 212.

Using a script to create database objects manually requires that you take one of the following actions.

- Grant the **db_owner** role to the database *user* in VCDB and in MSDB. See "Set Database Permissions by Using the dbo Schema and the db_owner Database Role," on page 207 and "Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role," on page 207.

- Grant the **VC_ADMIN_ROLE** to the database *user* in VCDB and in MSDB, and grant the **VC_USER_ROLE** to the database *user* in VCDB. See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206.

Prerequisites

Create the SQL Server database. You can create the SQL Server database manually or by using a script. See "Create a SQL Server Database and User for vCenter Server," on page 205

Procedure

1. Log in to a Microsoft SQL Server Management Studio session as *user_name* for a user account that you created on the vCenter Server and MSDB databases.
2. Locate the dbschema scripts in the vCenter Server installation package `/installation_directory/vCenter-Server/dbschema` directory.
3. Open the `sql` file through Microsoft SQL Server Management Studio and replace all occurrences of `$schema` with the schema name in the file `VCDB_mssql.SQL`.
4. Run the scripts in sequence on the database.

   The DBO user must own the objects created by these scripts. Open the scripts one at a time in Microsoft SQL Server Management Studio and press F5 to execute each script in the order shown here.

   ```
   VCDB_mssql.SQL
   load_stats_proc_mssql.sql
   purge_stat2_proc_mssql.sql
   purge_stat3_proc_mssql.sql
   purge_usage_stats_proc_mssql.sql
   stats_rollup1_proc_mssql.sql
   stats_rollup2_proc_mssql.sql
   stats_rollup3_proc_mssql.sql
   cleanup_events_mssql.sql
   delete_stats_proc_mssql.sql
   upsert_last_event_proc_mssql.sql
   load_usage_stats_proc_mssql.sql
   TopN_DB_mssql.sql
   calc_topn1_proc_mssql.sql
   calc_topn2_proc_mssql.sql
   calc_topn3_proc_mssql.sql
   calc_topn4_proc_mssql.sql
   clear_topn1_proc_mssql.sql
   clear_topn2_proc_mssql.sql
   clear_topn3_proc_mssql.sql
   clear_topn4_proc_mssql.sql
   rule_topn1_proc_mssql.sql
   rule_topn2_proc_mssql.sql
   rule_topn3_proc_mssql.sql
   rule_topn4_proc_mssql.sql
   process_license_snapshot_mssql.sql
   l_stats_rollup3_proc_mssql.sql
   l_purge_stat2_proc_mssql.sql
   l_purge_stat3_proc_mssql.sql
   l_stats_rollup1_proc_mssql.sql
   l_stats_rollup2_proc_mssql.sql
   VCDB_view_mssql.sql
   ```

5 (Optional) You can also run the following scripts to enable database health monitoring.

```
job_dbm_performance_data_mssql.sql
process_performance_data_mssql.sql
```

6 For all supported editions of Microsoft SQL Server (except Microsoft SQL Server 2005 Express and Microsoft SQL Server 2008 R2 Express), run these scripts to set up scheduled jobs on the database.

These scripts ensure that the SQL Server Agent service is running.

```
job_schedule2_mssql.sql
job_schedule3_mssql.sql
job_cleanup_events_mssql.sql
job_topn_past_day_mssql.sql
job_topn_past_week_mssql.sql
job_topn_past_month_mssql.sql
job_topn_past_year_mssql.sql
job_property_bulletin_mssql.sql
```

7 For all the procedures you created in Step 4, grant the execute privilege to the vCenter Server database.

```
grant execute on purge_stat2_proc to vCenter_db_user
grant execute on purge_stat3_proc to vCenter_db_user
grant execute on purge_usage_stat_proc to vCenter_db_user
grant execute on stats_rollup1_proc to vCenter_db_user
grant execute on stats_rollup2_proc to vCenter_db_user
grant execute on stats_rollup3_proc to vCenter_db_user
grant execute on cleanup_events_tasks_proc to vCenter_db_user
grant execute on delete_stats_proc to vCenter_db_user
grant execute on upsert_last_event_proc to vCenter_db_user
grant execute on load_usage_stats_proc to vCenter_db_user
grant execute on load_stats_proc to vCenter_db_user
grant execute on calc_topn1_proc to vCenter_db_user
grant execute on calc_topn2_proc to vCenter_db_user
grant execute on calc_topn3_proc to vCenter_db_user
grant execute on calc_topn4_proc to vCenter_db_user
grant execute on clear_topn1_proc to vCenter_db_user
grant execute on clear_topn2_proc to vCenter_db_user
grant execute on clear_topn3_proc to vCenter_db_user
grant execute on clear_topn4_proc to vCenter_db_user
grant execute on rule_topn1_proc to vCenter_db_user
grant execute on rule_topn2_proc to vCenter_db_user
grant execute on rule_topn3_proc to vCenter_db_user
grant execute on rule_topn4_proc to vCenter_db_user
grant execute on process_license_snapshot_proc to vCenter_db_user
grant execute on l_stats_rollup3_proc to vCenter_db_user
grant execute on l_purge_stat2_proc to vCenter_db_user
grant execute on l_purge_stat3_proc to vCenter_db_user
grant execute on l_stats_rollup1_proc to vCenter_db_user
grant execute on l_stats_rollup2_proc to vCenter_db_user
grant execute on process_temptable0_proc to vCenter_db_user
grant execute on process_temptable1_proc to vCenter_db_user
grant execute on process_temptable2_proc to vCenter_db_user
```

If you ran the script `process_performance_data_mssql.sql` in Step 4, grant the following execute privilege to the vCenter Server database.

```
grant execute on process_performance_data_proc to vCenter_db_user
```

8 On the machine on which you intend to install vCenter Server, create a DSN that points to the database server with the schema.

9 Run the vCenter Server installer.

10 If a database reinitialization warning message appears in the vCenter Server installer, select **Do not overwrite, leave my existing database in place** and continue the installation.

This message appears if you are using a database that has vCenter Server tables that were created by a previous installation. The message does not appear if the database is clean.

If you leave your existing database in place, you cannot join a Linked Mode group during the installation. You can join after the installation is complete. See "Join a Linked Mode Group After Installation," on page 296.

11 When prompted, provide the database user login.

Configure a SQL Server ODBC Connection

After you create a vCenter Server user, establish a connection with a SQL Server database. This connection is required to install a vCenter Server system.

If you use SQL Server for vCenter Server, do not use the master database.

See your Microsoft SQL ODBC documentation for specific instructions regarding configuring the SQL Server ODBC connection.

CAUTION If you are using a named instance of Microsoft SQL Server 2008 Standard Edition with vCenter Server, do not name the instance MSSQLSERVER. If you do, the JDBC connection does not work, and certain features, such as Performance Charts, are not available.

Prerequisites

- Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 194.
- Create a database using SQL Server Management Studio on the SQL Server. See "Create a SQL Server Database and User for vCenter Server," on page 205
- Set database permissions using one of the following options:
  - Option 1 (recommended): Follow the procedures in "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 206 and "Use a Script to Create a Microsoft SQL Server Database Schema and Roles," on page 208
  - Option 2 (alternative): Follow the procedures in "Set Database Permissions by Using the dbo Schema and the db_owner Database Role," on page 207 and "Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role," on page 207.

Procedure

1 On your vCenter Server system, select **Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Click the **System DSN** tab and do one of the following.

- To modify an existing SQL Server ODBC connection, select the connection from the System Data Source list and click **Configure**.
- To create a new SQL Server ODBC connection, click **Add**, select **SQL Native Client**, and click **Finish**.

3 Type an ODBC datastore name (DSN) in the **Name** text box.

For example, VMware vCenter Server.

4 (Optional) Type an ODBC DSN description in the **Description** text box.

5 Select the server name from the **Server** drop-down menu.

Type the SQL Server host name in the text box if it is not in the drop-down menu.

6 Select one of the authentication methods.

- **Integrate Windows authentication**. Optionally, enter the Service Principal Name (SPN).
- **SQL Server authentication**. Type your SQL Server login name and password.

7 Select the database created for the vCenter Server system from the **Change the default database to** menu.

8 Click **Finish**.

9 For SQL Server 2005 and SQL Server 2008 editions, test the data source by selecting **Test Data Source** and clicking **OK** from the **ODBC Microsoft SQL Server Setup** menu.

10 Verify that the SQL Agent is running on your database server.

Configure Microsoft SQL Server TCP/IP for JDBC

If the Microsoft SQL Server database has TCP/IP disabled and the dynamic ports are not set, the JDBC connection remains closed. The closed connection causes the vCenter Server statistics to malfunction. You can configure the server TCP/IP for JDBC.

This task applies to remote Microsoft SQL Server database servers. You can skip this task if your database is local.

Procedure

1 Select **Start > All Programs > Microsoft SQL Server > Configuration Tool > SQL Server Configuration Manager**.

2 Select **SQL Server Network Configuration > Protocols for***Instance name*.

3 Enable TCP/IP.

4 Open TCP/IP Properties.

5 On the **Protocol** tab, make the following entries.

Enabled	**Yes**
Listen All	**Yes**
Keep Alive	**30000**

6 On the **IP Addresses** tab, make the following selections.

Active	**Yes**
TCP Dynamic Ports	**0**

7 Restart the SQL Server service from **SQL Server Configuration Manager > SQL Server Services**.

8 Start the SQL Server Browser service from **SQL Server Configuration Manager > SQL Server Services**.

What to do next

Optionally, you can enable Database Monitoring for Microsoft SQL database users. Otherwise, install vCenter Server.

(Optional) Configure a Microsoft SQL Server Database User to Enable Database Monitoring

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime because of a lack of resources for the database server.

Database Monitoring for vCenter Server enables administrators to monitor the database server CPU, memory, I/O, data storage, and other environment factors for stress conditions. Statistics are stored in the vCenter Server Profile Logs.

You can enable Database Monitoring for a user before or after you install vCenter Server. You can also perform this procedure while vCenter Server is running.

Procedure

1 Log in to a SQL Server Management Studio session as the sysadmin (SA) or to a user account with sysadmin privileges.

2 Run the following SQL commands to grant additional permissions to vCenter Server database login:

```
usemaster
go
grant VIEW SERVER STATE to login name
go
```

vCenter Database Monitoring is enabled.

Configure Oracle Databases

To use an Oracle database for your vCenter Server repository, configure your database to work with vCenter Server.

Procedure

1 Configure an Oracle Database User on page 215

To use an Oracle database when you install vCenter Server, you must configure the database user.

2 Use a Script to Create a Local or Remote Oracle Database on page 216

When you use an Oracle database with vCenter Server, the database must have certain table spaces and privileges. To simplify the process of creating the database, you can run a script. You also can create the database manually.

3 (Optional) Use a Script to Create the Oracle Database Schema on page 216

The vCenter Server installer creates the schema during installation. For experienced database administrators who need more control over schema creation because of environmental constraints, you can optionally use a script to create your database schema.

4 Configure an Oracle Connection for Local Access on page 218

Configure a connection for local access if you install vCenter Server on the same system as the Oracle database.

5 Configure an Oracle Database Connection for Remote Access on page 218

Before a vCenter Server system can access the Oracle database remotely, you must configure an Oracle connection.

6 Connect to an Oracle Database Locally on page 219

Before a vCenter Server system can connect to an Oracle database locally, you must set up the connection.

7 (Optional) Configure an Oracle Database User to Enable Database Monitoring on page 220

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime because of a lack of resources for the database server.

Configure an Oracle Database User

To use an Oracle database when you install vCenter Server, you must configure the database user.

You can configure an Oracle database for vCenter Server either locally on the same Microsoft Windows machine as vCenter Server or remotely on a network-connected Linux, UNIX or Microsoft Windows host.

Prerequisites

Review the software requirements for vCenter Server with Oracle.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL command to create a vCenter Server database user with the correct permissions.

The script is located in the vCenter Server installation package */installation directory*/vpx/dbschema/DB_and_schema_creation_scripts_oracle.txt file.

In this example, the user name is VPXADMIN.

```
CREATE USER "VPXADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE
"VPX" ACCOUNT UNLOCK;
grant connect to VPXADMIN;
grant resource to VPXADMIN;
grant create view to VPXADMIN;
grant create sequence to VPXADMIN;
grant create table to VPXADMIN;
grant create materialized view to VPXADMIN;
grant execute on dbms_lock to VPXADMIN;
grant execute on dbms_job to VPXADMIN;
grant select on dba_tablespaces to VPXADMIN;
grant select on dba_temp_files to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant unlimited tablespace to VPXADMIN;
```

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.

NOTE Instead of granting `unlimited tablespace`, you can set a specific tablespace quota. The recommended quota is `unlimited` with a minimum of at least 500MB. To set an unlimited quota, use the following command.

```
alter user "VPXADMIN" quota unlimited on "VPX";
```

If you set a limited quota, monitor the remaining available tablespace to avoid the following error.

```
ORA-01536: space quota exceeded for tablespace '<tablespace>'
```

---

3 (Optional) After you have successfully installed vCenter Server with the Oracle database, you can revoke the following privileges.

```
revoke select on dba_tablespaces from VPXADMIN;
revoke select on dba_temp_files from VPXADMIN;
revoke select on dba_data_files from VPXADMIN;
```

You now have an Oracle database user that you can reference in the vCenter Server installer.

What to do next

Create the Oracle database, including all necessary table spaces and privileges.

Use a Script to Create a Local or Remote Oracle Database

When you use an Oracle database with vCenter Server, the database must have certain table spaces and privileges. To simplify the process of creating the database, you can run a script. You also can create the database manually.

When using the script, you can customize the location of the data and log files. The user created by this script does not follow any security policy. The passwords are provided only for convenience. Change the passwords as appropriate.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following script.

The script is located in the vCenter Server installation package `/installation directory/vpx/dbschema/DB_and_schema_creation_scripts_oracle.txt` file.

```
CREATE SMALLFILE TABLESPACE "VPX" DATAFILE '/u01/app/oracle/oradata/vcdb/vpx01.dbf'
SIZE 1G AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

For a Windows installation, change the directory path to the `vpx01.dbf` file.

You now have an Oracle database that you can use with vCenter Server.

What to do next

You can run a script to create the database schema.

(Optional) Use a Script to Create the Oracle Database Schema

The vCenter Server installer creates the schema during installation. For experienced database administrators who need more control over schema creation because of environmental constraints, you can optionally use a script to create your database schema.

To have the vCenter Server installer create your schema for you, see "Configure an Oracle Connection for Local Access," on page 218 or "Configure an Oracle Database Connection for Remote Access," on page 218, depending on your environment.

Prerequisites

Create the Oracle database and user. You can create the Oracle database and user manually or by using scripts.

Procedure

1 Open a SQL*Plus window with a user that has schema owner rights on the vCenter Server database.

2 Locate the dbschema scripts in the vCenter Server installation package `/installation directory/vpx/dbschema` directory.

3 In SQL*Plus, run the scripts in sequence on the database.

path is the directory path to the */installation directory*/vpx/dbschema folder.

```
@path/VCDB_oracle.SQL
@path/load_stats_proc_oracle.sql
@path/purge_stat2_proc_oracle.sql
@path/purge_stat3_proc_oracle.sql
@path/purge_usage_stats_proc_oracle.sql
@path/stats_rollup1_proc_oracle.sql
@path/stats_rollup2_proc_oracle.sql
@path/stats_rollup3_proc_oracle.sql
@path/cleanup_events_oracle.sql
@path/delete_stats_proc_oracle.sql
@path/load_usage_stats_proc_oracle.sql
@path/TopN_DB_oracle.sql
@path/calc_topn1_proc_oracle.sql
@path/calc_topn2_proc_oracle.sql
@path/calc_topn3_proc_oracle.sql
@path/calc_topn4_proc_oracle.sql
@path/clear_topn1_proc_oracle.sql
@path/clear_topn2_proc_oracle.sql
@path/clear_topn3_proc_oracle.sql
@path/clear_topn4_proc_oracle.sql
@path/rule_topn1_proc_oracle.sql
@path/rule_topn2_proc_oracle.sql
@path/rule_topn3_proc_oracle.sql
@path/rule_topn4_proc_oracle.sql
@path/process_license_snapshot_oracle.sql
@path/l_stats_rollup3_proc_oracle.sql
@path/l_purge_stat2_proc_oracle.sql
@path/l_purge_stat3_proc_oracle.sql
@path/l_stats_rollup1_proc_oracle.sql
@path/l_stats_rollup2_proc_oracle.sql
@path/process_temptable0_proc_oracle.sql
@path/process_temptable1_proc_oracle.sql
@path/process_temptable2_proc_oracle.sql
```

4 (Optional) You can also run the following scripts to enable database health monitoring.

```
job_dbm_performance_data_oracle.sql
process_performance_data_oracle.sql
```

5 For all supported editions of Oracle Server, run these scripts to set up scheduled jobs on the database.

```
@path/job_schedule2_oracle.sql
@path/job_schedule3_oracle.sql
@path/job_cleanup_events_oracle.sql
@path/job_topn_past_day_oracle.sql
@path/job_topn_past_week_oracle.sql
@path/job_topn_past_month_oracle.sql
@path/job_topn_past_year_oracle.sql
@path/job_property_bulletin_oracle.sql
```

You now have a database schema that is compatible with vCenter Server.

6 On the machine that you are installing vCenter Server on, create a DSN that points to the database server that has the schema.

7 Run the vCenter Server installer.

8 If a database reinitialization warning message appears in the vCenter Server installer, select **Do not overwrite, leave my existing database in place** and continue the installation.

This message appears if you are using a database that has vCenter Server tables that were created by a previous installation. The message does not appear if the database is clean.

If you leave your existing database in place, you cannot join a Linked Mode group during the installation. You can join after the installation is complete. See "Join a Linked Mode Group After Installation," on page 296.

9 When prompted, provide the database user login.

The Oracle dadtabase schema is created.

Configure an Oracle Connection for Local Access

Configure a connection for local access if you install vCenter Server on the same system as the Oracle database.

Prerequisites

Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 194. If you do not prepare your database correctly, the vCenter Server installer displays error and warning messages.

Procedure

1 Download Oracle 10g or Oracle 11g from the Oracle Web site.

2 Install Oracle 10g or Oracle 11g, and create a database.

3 Configure the TNS Service Name option in the ODBC DSN.

The TNS Service Name is the net service name for the database to which you want to connect. You can find the net service name in the `tnsnames.ora` file located in the `NETWORK\ADMIN` folder in the Oracle database installation location.

The database is configured for local access.

Configure an Oracle Database Connection for Remote Access

Before a vCenter Server system can access the Oracle database remotely, you must configure an Oracle connection.

Prerequisites

Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 194. If you do not prepare your database correctly, the vCenter Server installer displays error and warning messages.

Procedure

1 Install the Oracle client on the vCenter Server system machine.

2 Download and install the ODBC driver.

3 Create a new tablespace for a vCenter Server system using a SQL statement such as the following statement.

```
CREATE TABLESPACE "VPX" DATAFILE 'C:\Oracle\ORADATA\VPX\VPX.dat' SIZE 1000M AUTOEXTEND ON NEXT
500K;
```

4 Create a user, such as vpxAdmin, for accessing the tablespace through ODBC.

```
CREATE USER vpxAdmin IDENTIFIED BY vpxadmin DEFAULT TABLESPACE vpx;
```

5 Grant permissions to the user, in one of the following ways.

- Grant **dba** permission to the user.
- Grant the following permissions to the user.

```
grant connect to user
grant resource to user
grant create view to user
grant create sequence to user
grant create table to user
grant create materialized view to user
grant execute on dbms_lock to user
grant execute on dbms_job to user
grant unlimited tablespace to user # To ensure space is sufficient
```

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.

6 Use a text editor or the Net8 Configuration Assistant to edit the `tnsnames.ora` file located in the directory `C:\Oracle\Oraxx\NETWORK\ADMIN`, where `xx` is either 10g or 11g.

Add the following entry, where `HOST` is the managed host to which the client must connect.

```
VPX =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP)(HOST=vpxd-Oracle)(PORT=1521))
   )
(CONNECT_DATA =
(SERVICE_NAME = VPX)
   )
   )
```

7 Configure the TNS Service Name option in the ODBC DSN.

The TNS Service Name is the net service name for the database to which you want to connect, in this case, VPX. You can find the net service name in the `tnsnames.ora` file.

Connect to an Oracle Database Locally

Before a vCenter Server system can connect to an Oracle database locally, you must set up the connection.

Procedure

1 Create a new tablespace for a vCenter Server system using a SQL statement such as the following statement.

```
CREATE TABLESPACE "VPX" DATAFILE 'C:\Oracle\ORADATA\VPX\VPX.dat' SIZE 1000M AUTOEXTEND ON NEXT
500K;
```

2 Create a user, such as vpxAdmin, for accessing the tablespace through ODBC.

```
CREATE USER vpxAdmin IDENTIFIED BY vpxadmin DEFAULT TABLESPACE vpx;
```

3 Grant permissions to the user, in one of the following ways.

- Grant **dba** permission to the user.
- Grant the following permissions to the user.

```
grant connect to user
grant resource to user
grant create view to user
grant create sequence to user
grant create table to user
grant create materialized view to user
grant execute on dbms_lock to user
grant execute on dbms_job to user
grant unlimited tablespace to user # To ensure space is sufficient
```

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.

4 Create an ODBC connection to the database.

The following code shows example settings.

```
Data Source Name: VMware vCenter Server  TNS Service Name: VPX  User Id: vpxAdmin
```

You now have a database that you can connect to locally.

What to do next

Optionally, you can enable Database Monitoring for Oracle database users. Otherwise, install vCenter Server.

(Optional) Configure an Oracle Database User to Enable Database Monitoring

vCenter Server Database Monitoring captures metrics that enable the administrator to assess the status and health of the database server. Enabling Database Monitoring helps the administrator prevent vCenter downtime because of a lack of resources for the database server.

Database Monitoring for vCenter Server enables administrators to monitor the database server CPU, memory, I/O, data storage, and other environment factors for stress conditions. Statistics are stored in the vCenter Server Profile Logs.

Enable Database Monitoring for a user before or after you install vCenter Server. You can perform this procedure while vCenter Server is running.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL commands to grant additional permissions to the vCenter Server database user:

```
grant select on v_$system_event to user;
grant select on v_$sysmetric_history to user;
grant select on v_$sysstat to user;
grant select on dba_data_files to user;
grant select on v_$loghist to user;
```

vCenter Database Monitoring is enabled.

Before You Install vCenter Server 10

You can install vCenter Server on a physical system or on a virtual machine running on an ESXi host. You can also download the VMware vCenter Server Appliance, a preconfigured Linux-based virtual machine optimized for running vCenter Server.

This chapter includes the following topics:

Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server

Before installing vCenter Single Sign-On, Inventory Service, and vCenter Server, review the prerequisites.

Prerequisites for Understanding and Preparing for the Installation Process

- vCenter Server 5.1 requires vCenter Single Sign-On and Inventory Service. You must install these components in this order: vCenter Single Sign-On, Inventory Service, and vCenter Server. Review the topics in the section "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224
- Review the release notes for known issues or special installation notes.

- Gather the information that the vCenter Single Sign-On, Inventory Service , and vCenter Server installation wizards require. See "Required Information for Installing or Upgrading vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 237.
- Decide whether the vCenter Server instance will be a standalone instance or in a Linked Mode group. See "Creating vCenter Server Linked Mode Groups," on page 293.
- Download the vCenter Server 5.1 installer from the VMware Web site.

System Prerequisites

- Verify that your system meets the requirements listed in "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33 and "vCenter Server Software Requirements," on page 37, and that the required ports are open, as discussed in "Required Ports for vCenter Server," on page 39.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 232.
- Review the Windows Group Policy Object (GPO) password policy for your system machines. The Single Sign On installation requires you to enter passwords that comply with GPO password policy.
- Verify that the DNS name of the vCenter Server host machine matches the actual computer name.
- Verify that the host name of the machine that you are installing vCenter Server on complies with RFC 952 guidelines.
- The installation path of vCenter Server must be compatible with the installation requirements for Microsoft Active Directory Application Mode (ADAM/AD LDS). The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).
- Verify that the host machine computer name is no more than 15 characters.
- Verify that the system on which you are installing vCenter Server is not an Active Directory domain controller.
- On each system that is running vCenter Server, verify that the domain user account has the following permissions:
  - **Member of the Administrators group**
  - **Act as part of the operating system**
  - **Log on as a service**
- vCenter Server requires the Microsoft .NET 3.5 SP1 Framework. If your system does not have it installed, the vCenter Server installer installs it. The .NET 3.5 SP1 installation might require Internet connectivity to download more files.
- If the system that you use for your vCenter Server installation belongs to a workgroup rather than a domain, not all functionality is available to vCenter Server. If assigned to a workgroup, the vCenter Server system is not able to discover all domains and systems available on the network when using some features. To determine whether the system belongs to a workgroup or a domain, right-click **My Computer**. Click **Properties** and click the **Computer Name** tab. The **Computer Name** tab displays either a Workgroup label or a Domain label.
- Verify that the NETWORK SERVICE account has read permission on the folder in which vCenter Server is installed and on the HKLM registry.
- During the installation, verify that the connection between the machine and the domain controller is working.

- Before the vCenter Server installation, in the Administrative Tools control panel of the vCenter Single Sign-On instance that you will register vCenter Server to, verify that the vCenter Single Sign-On and RSA SSPI services are started.
- You must log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Network Prerequisites

- Verify that the fully qualified domain name (FQDN) of the system where you will install vCenter Server is resolvable. To check that the FQDN is resolvable, type **`nslookup`** ***`your_vCenter_Server_fqdn`*** at a command line prompt. If the FQDN is resolvable, the **`nslookup`** command returns the IP and name of the domain controller machine.
- Verify that DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server. When you install vCenter Server, the installation of the web server component that supports the vSphere Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server from its IP address. Reverse lookup is implemented using PTR records. To create a PTR record, see the documentation for your vCenter Server host operating system.
- Verify that no Network Address Translation (NAT) exists between the vCenter Server system and the hosts it will manage.
- Install vCenter Server, like any other network server, on a machine with a fixed IP address and well known DNS name, so that clients can reliably access the service. Assign a static IP address and host name to the Windows server that will host the vCenter Server system. This IP address must have a valid (internal) domain name system (DNS) registration. Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Clients. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Clients. If you use DHCP instead of a static IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Ping the computer name to test this connection. For example, if the computer name is `host-1.company.com`, run the following command in the Windows command prompt:

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

  If you can ping the computer name, the name is updated in DNS.
- For the vCenter Single Sign-On installer to automatically discover Active Directory identity sources, verify that the following conditions are met.
  - The Active Directory identity source must be able to authenticate the user who is logged in to perform the Single Sign-On installation.
  - The DNS of the Single Sign-On Server host machine must contain both lookup and reverse lookup entries for the domain controller of the Active Directory. For example, pinging *mycompany.com* should return the domain controller IP address for *mycompany*. Similarly, the `ping -a` command for that IP address should return the domain controller hostname. Avoid trying to correct name resolution issues by editing the hosts file. Instead, make sure that the DNS server is correctly set up.
  - The system clock of the Single Sign-On Server host machine must be synchronized with the clock of the domain controller.

Database Prerequisites

- Verify that your vCenter Server database meets the database requirements. See "vCenter Server Database Configuration Notes," on page 194 and Chapter 9, "Preparing vCenter Server Databases," on page 193.
- Create a vCenter Server database, unless you plan to install the bundled database.
- Create a vCenter Single Sign-On database, unless you plan to install the bundled database.

- If you are using an existing database for Single Sign On, you must create a database user (RSA_USER) and database administrator (RSA_DBA) to use for the Single Sign On database installation and setup. To create these users, run the script `rsaIMSLite`*`DBName`*`SetupUsers.sql`. The script is included in the vCenter Server installer download package, at *`vCenter Server Installation directory`*`\SSOServer`.
- If you are using an existing database with your vCenter Single Sign-On installation or upgrade, make sure that the table spaces are named RSA_DATA and RSA_INDEX. Any other table space names will cause the vCenter Single Sign-On Installation to fail.
- If you are using an existing database for Single Sign-On, to ensure that table space is created for the database, run the script `rsaIMSLite<DBName>SetupTablespaces.sql`. The script is included in the vCenter Server installer download package, at *`vCenter Server Installation directory`*`\Single Sign On\DBScripts\SSOServer\Schema\`*`your_existing_database`*. You can run this script prior to the installation, or during the installation, when you are prompted by the installer. You can leave the installer to run the script, and resume the installer after you run the script.

How vCenter Single Sign On Affects vCenter Server Installation and Upgrades

vSphere 5.1 introduces the vCenter Single Sign On service as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation.

Authentication by vCenter Single Sign-On makes the VMware cloud infrastructure platform more secure by allowing the vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

For information about configuring vCenter Single Sign On, see *vSphere Security*.

How vCenter Single Sign-On Affects New vCenter Server Installations

In vSphere versions before vSphere 5.1, vCenter Server was installed in a single operation that also silently installed the Inventory Service on the same host machine.

For small vSphere deployments, vCenter Server 5.1 provides a vCenter Server Simple Install option that installs vCenter Single Sign-On, Inventory Service, and vCenter Server on the same host or virtual machine.

Alternatively, to customize the location and setup of each component, you can install the components separately by selecting the individual installation options, in the following order: vCenter Single Sign-On, Inventory Service, and vCenter Server. Each component can be installed in a different host or virtual machine.

For the first installation of vCenter Server with vCenter Single Sign-On, you must install all three components, Single Sign-On Server, Inventory Service, and vCenter Server, in the vSphere environment. In subsequent installations of vCenter Server in your environment, you do not need to install Single Sign-On. One Single Sign-On server can serve your entire vSphere environment. After you install vCenter Single Sign-On once, you can connect all new vCenter Server instances to the same authentication server. However, you must install a Inventory Service instance for each vCenter Server instance.

How vCenter Single Sign-On Affects vCenter Server Upgrades

When you upgrade to vCenter Server 5.1, the upgrade process installs vCenter Single Sign-On first and then upgrades vCenter Server.

In upgrades to vCenter Server versions earlier than vCenter Server 5.1, both the local operating system users and Active Directory users that are registered with vCenter Server before the upgrade continue to work with the upgraded vCenter Server. This behavior changes in vCenter Server 5.1.

In vCenter Server 5.1, if vCenter Single Sign-On is running on a virtual machine or physical machine that is joined to an Active Directory domain, Single Sign-On will automatically discover the existing Active Directory domain and add it as an identity source during the Single Sign-On installation process. If Single Sign-On is not running on a virtual machine or physical machine that is in the same domain as Active Directory, you must use the vSphere Web Client to log in to vCenter Server and add the Active Directory domain to Single Sign-On.

If you install vCenter Single Sign-On and vCenter Server on the same physical machine or virtual machine, Single Sign-On recognizes existing local operating system users. After the upgrade, you can log in to vCenter Server with a registered local operating system user ID.

If you install vCenter Single Sign-On and vCenter Server on different hosts or virtual machines, the former local operating system users who managed login access to vCenter Server are not available to Single Sign-On.

When you install vCenter Single Sign-On in multisite mode or clustered high availability mode, all pre-upgrade permissions for local operating system users are lost. In vCenter Server 5.1, the term "local operating system users" refers to those local users in the Single Sign-On host machine instead of the vCenter Server host machine or virtual machine.

After the upgrade, if no super administrator remains (the administrative user or group for the root folder), you must provide a valid user or group to be used as super administrator during installation. This situation can occur due to changes in user stores from pre-5.1 to 5.1 versions of vSphere.

vCenter Single Sign-On Deployment Modes

vCenter Server provides several ways to deploy vCenter Single Sign-On to best serve your vSphere environment

You can deploy vCenter Single Sign-On in one of three modes.

Basic Basic mode installs a standalone version of vCenter Single Sign-On. Multiple vCenter Server and Inventory Service instances can point to it. If the Single Sign-On server or the virtual machine hosting the server fails, administrators cannot access vCenter Server, but ESXi hosts continue to function normally. Multiple Active Directory and OpenLDAP instances can be added as identity sources.

High Availability Cluster Cluster mode installs two or more vCenter Single Sign-On instances in high availability mode. All instances use the same database and point to the same identity sources. Single Sign-On administrator users, when connected to vCenter Server through the vSphere Web Client, will see the primary Single Sign-On instance.

Multisite Multisite mode is designed for deployments with multiple physical locations. Installing a Single Sign-On instance at each site allows fast access to local authentication-related services. Each Single Sign-On instance is connected to the local instances of the AD (LDAP) servers and has its own database with local users and groups. In each datacenter, you can install Single Sign-On in standalone or clustered mode, pointing to the identity sources in that location.

Multisite deployment is useful when a single administrator needs to administer vCenter Server instances that are deployed on geographically dispersed sites. To view all vCenter Server instances from a single vSphere Web Client, you must configure the vCenter Server instances in Linked Mode.

NOTE Multisite Single Sign-On deployment is designed only for faster local access to authentication-related services. It does not provide failover between Single Sign-On servers on different sites. When the Single Sign-On instance on one site fails, its role is not taken over by a peer Single Sign-On instance on another site. All authentication requests on the failed site will fail, even if peer sites are fully functional.

In multisite Single Sign-On deployments, each site is represented by one Single Sign-On instance: one Single Sign-On server, or a high-availability cluster. The Single Sign-On site entry point is the machine that other sites communicate with. This is the only machine that needs to be visible from the other sites. In a clustered deployment, the entry point of the site is the machine where the load balancer is installed.

You can install the Single Sign-On nodes in a multisite deployment in any order. The Single Sign-On installer uses the terms primary and secondary only to distinguish between the node that is installed first and any node that is installed later and points to a previously installed node. Any node that is installed after the primary node can point to any node that is already installed. For example, the third node can point to either the first or second node.

For example, consider a corporation MyCompany, with offices in San Francisco, New York, and London. The New York site is the headquarters and connects with both the London and San Francisco sites. The London and San Francisco sites do not connect with each other. The MyCompany multisite Single Sign-On deployment would proceed in the following steps.

1. The administrators in London set up the first Single Sign-On instance.
2. The New York IT team sets up the second Single Sign-On instance, pointing it to the London instance.
3. The San Francisco IT team sets up the third Single Sign-On instance, pointing it to the New York instance.

vCenter Server instances in linked mode can be connected to different physical Single Sign-On servers, but must be connected to a single logical Single Sign-On server. A single logical Single Sign-On server can take any of the following forms.

- A single physical Single Sign-On server.
- Two nodes of a cluster. Effectively this is the same as a single physical Single Sign-On server because the nodes use the same Single Sign-On database.
- Two nodes in multisite mode.

vCenter Single Sign On Components

vCenter Single Sign On includes these components: STS (Security Token Service), an administration server, vCenter Lookup Service, and the RSA SSPI service.

When you install vCenter Single Sign-On, the following components are deployed.

STS (Security Token Service)	The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens pass information about a system user between an identity provider and a web service. This service enables a user who has logged on through vCenter Single Sign-On to use multiple web-service delivered applications without authenticating to each one.
Administration server	The Administration Server configures the vCenter Single Sign-On server and manages users and groups.
vCenter Lookup Service	The Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely.
RSA SSPI service	The Security Support Provider Interface is a Microsoft Windows-based API used to perform authentication against Security Support Providers such as NTLM and Kerberos.

vCenter Lookup Service

vCenter Lookup Service is a component of vCenter Single Sign On. Lookup Service registers the location of vSphere components so they can securely find and communicate with each other.

The vCenter Single Sign-On installer also deploys the VMware Lookup Service on the same address and port. The Lookup Service enables different components of vSphere to find one another in a secure way. When you install vCenter Server components after vCenter Single Sign-On, you must provide the Lookup Service URL. The Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server are registered in Lookup Service so other vSphere components, like the vSphere Web Client, can find them.

Setting the vCenter Server Administrator User

In vCenter Server 5.1 with vCenter Single Sign On, the way you set the vCenter Server administrator user depends on your vCenter Single Sign On deployment.

In vSphere versions before vSphere 5.1, vCenter Server administrators are the users that belong to the local operating system administrators group.

In vSphere 5.1, when you install vCenter Server, you must provide the default (initial) vCenter Server administrator user or group. For small deployments where vCenter Server and vCenter Single Sign-On are deployed on the same host machine, you can designate the local operating system group Administrators as vCenter Server administrative users. This option is the default. This behavior is unchanged from vCenter Server 5.0.

For larger installations, where vCenter Single Sign-On and vCenter Server are deployed on different hosts, you cannot preserve the same behavior as in vCenter Server 5.0. Instead, assign the vCenter Server administrator role to a user or group from an identity source that is registered in the vCenter Single Sign-On server: Active Directory, OpenLDAP, or the system identity source.

Adding Active Directory and OpenLDAP Domains to vCenter Server 5.1

In vCenter Server versions earlier than vCenter Server 5.1, vCenter Server adds Active Directory domains that the vCenter Server host or virtual machine is part of. In vCenter Server 5.1, vCenter Single Sign-On discovers those Active Directory domains that the vCenter Single Sign-On host or virtual machine is part of.

vCenter Single Sign-On adds those discovered Active Directory domains. Unlike earlier vCenter Server versions, which permit only one Active Directory domain at a time to be configured for vCenter Server, in vCenter Server 5.1 with Single Sign-On, you can add multiple Active Directory domains.

If you use Active Directory in your infrastructure and you want the Single Sign-On installer to add Active Directory automatically as a Single Sign-On identity source, the following requirements apply:

- You must log in as a domain user when you install Single Sign-On.
- You must install Single Sign-On on a machine joined to the Active Directory domain. In this case, all machines on which Single Sign-On servers will be installed must be joined to the same domain. The domain controllers might be different, but the Single Sign-On server will discover and add the local one.
- On the Single Sign-On host machine, the Active Directory machine account must have read permissions on the entire Active Directory and on the user and group attributes of the Active Directory.

vCenter Single Sign-On can also add multiple OpenLDAP domains, and you can configure vCenter Server to be available to users who are registered with these OpenLDAP repositories, enabling you to manage vCenter Server access without Active Directory.

For more information about vCenter Single Sign-On, see *vSphere Security*.

Authenticating to the vCenter Server 5.1 Environment

In vCenter Server 5.1, users authenticate through vCenter Single Sign On.

In vCenter Server versions earlier than vCenter Server 5.1, when a user connects to vCenter Server, vCenter Server authenticates the user by validating the user against an Active Directory domain or the list of local operating system users.

Because vCenter Server now has its own vCenter Single Sign-On server, you must create Single Sign-On users to manage the Single Sign-On server. These users might be different from the users that administer vCenter Server.

The default vCenter Single Sign-On administrator user ID is admin@System-Domain. You can create Single Sign-On administrator users with the Single Sign-On administration tool in the vSphere Web Client. You can associate the following permissions with these users: Basic, Regular, and Administrator.

Users can log in to vCenter Server with the vSphere Client or the vSphere Web Client.

- Using the vSphere Client, the user logs in to each vCenter Server separately. All linked vCenter Server instances are visible on the left pane of the vSphere Client. The vSphere Client does not show vCenter Server systems that are not linked to the vCenter Server that the user logged in to unless the user connects to those vCenter Server systems explicitly. This behavior is unchanged from vCenter Server versions earlier than version 5.1.
- Using the vSphere Web Client, users authenticate to vCenter Single Sign-On, and are connected to the vSphere Web Client. Users can view all the vCenter Server instances that the user has permissions on. After users connect to vCenter Server, no further authentication is required. The actions users can perform on objects depend on the user's vCenter Server permissions on those objects.

For vCenter Server versions earlier than vCenter Server 5.1, you must explicitly register each vCenter Server system with the vSphere Web Client, using the vSphere Web Client Administration Application.

For more information about vCenter Single Sign On, see *vSphere Security*.

How vCenter Single Sign-On Deployment Scenarios Affect Log In Behavior

The way that you deploy vCenter Single Sign-On and the type of user who installs vCenter Single Sign-On affects which administrator user accounts have privileges on the Single Sign-On server and on vCenter Server.

During the vCenter Server installation process, certain users are granted privileges to log in to vCenter Server and certain users are granted privileges to manage vCenter Single Sign-On. The vCenter Server administrator might not be the same user as the vCenter Single Sign-On administrator. This means that when you log in to the vSphere Web Client as the default Single Sign-On administrator (admin@System-Domain), you might not see any vCenter Server systems in the inventory. The inventory appears to be empty because you see only the systems upon which you have privileges in the vSphere Web Client.

This also means that when you log in to the vSphere Web Client as the default vCenter Server administrator, you might not see the vCenter Single Sign-On configuration tool. The configuration tool is not present because only the default vCenter Single Sign-On Administrator (admin@System-Domain) is allowed to view and manage vCenter Single Sign-On after installation. The Single Sign-On administrator can create additional administrator users if necessary.

Login Behavior When You Use vCenter Simple Install

The vCenter Simple Install process installs vCenter Single Sign-On, the Inventory Service, and vCenter Server on one system. The account you use when you run the Simple Install process affects which users have privileges on which components.

When you log in as a domain account user or local account user to install vCenter Server using vCenter Simple Install, the following behavior occurs upon installation.

- By default, users in the local operating system Administrators group can log in to the vSphere Web Client and vCenter Server. These users cannot configure Single Sign-On or view the Single Sign-On management interface in the vSphere Web Client.
- By default, the vCenter Single Sign-On administrator user is admin@System-Domain. This user can log in to the vSphere Web Client to configure Single Sign-On and add accounts to manage Single Sign-On if necessary. This user cannot view or configure vCenter Server.
- If you are logged in as a domain account user, the default Active Directory identity sources are discovered automatically during vCenter Single Sign On installation. If you are logged in as a local account user, Active Directory identity sources are not discovered automatically during vCenter Single Sign On installation.
- The local operating system (localos or *hostname*) users are added as an identity source.

Login Behavior When You Deploy vCenter Single Sign-On as a Standalone Server

Deploying vCenter Single Sign-On in Basic mode means that a standalone version of vCenter Single Sign-On is installed on a system. Multiple vCenter Server, Inventory Service, and vSphere Web Client instances can point to this standalone version of vCenter Single Sign-On.

In this deployment scenario, the installation process grants admin@System-Domain vCenter Server privileges by default. In addition, the installation process creates the user admin@System-Domain to manage vCenter Single Sign-On.

Note When you install vCenter Server components with separate installers, you can choose which account or group can log in to vCenter Server upon installation. Specify this account or group on the Single Sign-On Information page of the installer, in the following text box: **vCenter Server administrator recognized by vCenter Single Sign-On**. For example, to grant a group of domain administrators permission to log in to vCenter Server, type of name of the domain administrators group, such as Domain Admins@VCADSSO.LOCAL.

In high availablity and multisite Single Sign-On modes, there is no local operating system identity source. Therefore, it will not work if you enter **`Administrators`** or **`Administrator`** in the text box **vCenter Server administrator recognized by vCenter Single Sign-On**. **`Administrators`** is treated as the local operating system group Administrators, and **`Administrator`** is treated me as local operating system user Administrator.

Installing in Basic Mode as Domain Account User

When you log in as a domain account user to install vCenter Single Sign-On in basic mode, on a separate system from the Inventory Service and vCenter Server, the following behavior occurs upon installation.

- By default, the user admin@System-Domain can log in to the vSphere Web Client and vCenter Server.
- The default Active Directory identity sources are discovered.
- The local operating system (localos or *hostname*) users are added as an identity source.

Installing in Basic Mode as Local Account User

When you log in as a local account user to install vCenter Single Sign-On in basic mode, on a separate system from the Inventory Service and vCenter Server, the following behavior occurs upon installation.

- By default, the user admin@System-Domain can log in to the vSphere Web Client and vCenter Server.
- Active Directory identity sources are not discovered.
- The local operating system (localos or *hostname*) users are added as an identity source.

Login Behavior When You Install a Cluster of vCenter Single Sign-On Instances

Deploying vCenter Single Sign-On as a cluster means that two or more instances of vCenter Single Sign-On are installed in high availability mode. vCenter Single Sign-On high availability mode is not the same as vSphere HA. All instances of vCenter Single Sign-On use the same database and point to the same identity sources. Single Sign-On administrator users see the primary Single Sign-On instance when they connect to vCenter Server through the vSphere Web Client.

In this deployment scenario, the installation process grants admin@System-Domain vCenter Server privileges by default. In addition, the installation process creates the user admin@System-Domain to manage vCenter Single Sign-On.

NOTE When you install vCenter Server components with separate installers, you can choose which account or group can log in to vCenter Server upon installation. Specify this account or group on the Single Sign-On Information page of the installer, in the following text box: **vCenter Server administrator recognized by vCenter Single Sign-On**. For example, to grant a group of domain administrators permission to log in to vCenter Server, type of name of the domain administrators group, such as Domain Admins@VCADSSO.LOCAL.

In high availablity and multisite Single Sign-On modes, there is no local operating system identity source. Therefore, it will not work if you enter **`Administrators`** or **`Administrator`** in the text box **vCenter Server administrator recognized by vCenter Single Sign-On**. **`Administrators`** is treated as the local operating system group Administrators, and **`Administrator`** is treated me as local operating system user Administrator.

When you log in as a domain account user or local account user to install vCenter Single Sign-On in cluster mode, on a separate system from the Inventory Service and vCenter Server, the following behavior occurs upon installation.

- By default, the user admin@System-Domain can log in to the vSphere Web Client and vCenter Server.
- If you are logged in as a domain account user, the default Active Directory identity sources are discovered. If you are logged in as a local account user, Active Directory identity sources are not discovered.

Identity Sources for vCenter Server with vCenter Single Sign On

vCenter Server 5.1 with vCenter Single Sign On adds support for several new types of user repository.

vCenter Server versions earlier than version 5.1 supported Active Directory and local operating system users as user repositories. vCenter Server 5.1 supports the following types of user repositories as identity sources.

- Active Directory.
- OpenLDAP.
- Local operating system.
- System.

vCenter Single Sign-On identity sources are managed by Single Sign-On administrator users. You can attach multiple identity sources from each type to a single Single Sign-On server.

Each identity source has a name that is unique within the scope of the corresponding Single Sign-On server instance. There is always exactly one System identity source, named System-Domain.

There can be at most one local operating system identity source. On Linux systems, the identity source label is localOS. On Windows systems, the identity source label is the system's host name. The local operating system identity source can exist only in non-clustered Single Sign-On server deployments.

You can attach remote identity sources to a Single Sign-On server instance. Remote identity sources are limited to any of Active Directory, and OpenLDAP server implementations.

During Single Sign On installation, the installer can automatically discover Active Directory identity sources, if your system meets the appropriate prerequisites. See the section "Network Prerequisites" in "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

For more information about vCenter Single Sign On, see *vSphere Security*.

Synchronizing Clocks on the vSphere Network

Before you install vCenter Single Sign On, install the vSphere Web Client, or deploy the vCenter Server appliance, make sure all machines on the vSphere network have their clocks synchronized.

If the clocks on vCenter Server network machines are not synchronized, SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines. Unsynchronized clocks can result in authentication problems, which can cause the vSphere Web Client installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

Synchronize ESX and ESXi Clocks with a Network Time Server

Before you install vCenter Single Sign On, the vSphere Web Client, or the vCenter Server appliance, make sure all machines on the vSphere network have their clocks synchronized.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Select the **Manage** tab.

4 Select **Settings**.

5 Select **Time Configuration**.

6 Click **Edit**.

7 Select **Use Network Time Protocol (Enable NTP Client)**.

8 Set the NTP Service Status and NTP Service Startup Policy.

9 Enter the IP addresses of the NTP servers to synchronize with.

The host synchronizes with the NTP servers as specified in your settings.

Synchronize the vCenter Server Appliance Clock with an NTP Server

Before you deploy the vCenter Server Appliance or install vCenter Single Sign On on Windows, make sure all machines on the network have their clocks synchronized. Unsynchonized clocks can cause installation and authentication errors.

On systems joined to a Windows domain, the vCenter Server Appliance clock is synchronized automatically with the domain controller. On other systems, you can enable synchronizing the clock through VMware Tools. See the *Installing and Configuring VMware Tools Guide*. As an alternative, you can use this procedure.

Procedure

1 Log into the vCenter Server Appliance as root.

2 From a command line, enter the following commands to configure and start an NTP client.

```
yast2 ntp-client add server=your_chosen_time_server
yast2 ntp-client enable
```

3 Enter the following command to request immediate synchronization with the time server.

```
sntp -P no -r your_chosen_time_server
```

The vCenter Server Appliance clock is synchronized with the NTP server.

Configure a Windows NTP Client for Network Clock Synchronization

The clocks of all servers on the vSphere network must be synchronized. You can configure a Windows NTP client as a source for clock synchronization on Windows servers.

Use the registry editor on the Windows server to make the configuration changes.

Procedure

1 Enable NTP mode.

   a Go to the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

   b Set the Type value to **NTP**.

2 Enable the NTP client.

   a Go to the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

   b Set the AnnounceFlags value to **5**.

3 Enter the upstream NTP servers to synchronize from.

   a Go to the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders.

   b Set the NtpServer value to a list of at least three NTP servers.

   For example, you might set the value to 0x1 1.pool.ntp.org,0x1 2.pool.ntp.org,0x1 3.pool.ntp.org.

4 Specify a 150-minute update interval.

   a Go to the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient,

   b Set the SpecialPollInterval value to **900**.

5 Restart the W32time service for the changes to take effect.

Using a User Account for Running vCenter Server

You can use the Microsoft Windows built-in system account or a user account to run vCenter Server. With a user account, you can enable Windows authentication for SQL Server, and it provides more security.

The user account must be an administrator on the local machine. In the installation wizard, you specify the account name as *DomainName**Username*. You must configure the SQL Server database to allow the domain account access to SQL Server.

The Microsoft Windows built-in system account has more permissions and rights on the server than the vCenter Server system needs, which can contribute to security problems.

For SQL Server DSNs configured with Windows authentication, use the same user account for the VMware VirtualCenter Management Webservices service and the DSN user.

If you do not plan to use Microsoft Windows authentication for SQL Server or you are using an Oracle or DB2 database, you might still want to set up a local user account for the vCenter Server system. The only requirement is that the user account is an administrator on the local machine.

NOTE If you install an instance of vCenter Server as a local system account on a local SQL Server database with Integrated Windows NT Authentication, and you add an Integrated Windows NT Authentication user to the local database server with the same default database as vCenter Server, vCenter Server might not start. See "vCenter Server Fails to Start When Installed as a Local System Account on a Local SQL Server Database with Integrated Windows NT Authentication," on page 234.

vCenter Server Fails to Start When Installed as a Local System Account on a Local SQL Server Database with Integrated Windows NT Authentication

vCenter Server is installed as a local system account on a local SQL Server database with Integrated Windows NT Authentication. When you add an Integrated Windows NT Authentication user to the local database server, vCenter Server fails to start.

Problem

If you install an instance of vCenter Server as a local system account on a local SQL Server database with Integrated Windows NT Authentication, and you add an Integrated Windows NT Authentication user to the local database server with the same default database as vCenter Server, vCenter Server fails to start.

Solution

- Take one of the following actions.
  - Remove the Integrated Windows NT Authentication user from the local SQL database server.
  - Change the default database for the local system user account to the vCenter Server database for the SQL Server user account setup.

Installing vCenter Server on IPv6 Machines

vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to vCenter Server system in an IPv6 environment you must use the fully qualified domain name (FQDN) or host name of the vCenter Server.

The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

JDBC URL Formats for the vCenter Server Database

The vCenter Server installer generates and validates the JDBC URL for the vCenter Server database. If the installer fails to connect to the database using the generated JDBC URL, the installer will prompt you to specify the JDBC URL.

JDBC URL Notes for All Databases

NOTE The domain name cannot contain the exclamation point character (!). Java interprets the exclamation point as a jar file separator.

JDBC URL Formats for Microsoft SQL Server Databases

For Microsoft SQL Server databases, you can use the following example JDBC URLs as a model:

- Connect to default (unnamed) SQL Server instance by host name:

  jdbc:sqlserver://*host*;databaseName=*database*

- Connect to named instance by host name and instance name:

  jdbc:sqlserver://*host*;instanceName=*instance*;databaseName=*database*

- Connect to SQL Server by host name and port:

  jdbc:sqlserver://*host*:*port*;databaseName=*database*

- Connect by port:

  jdbc:sqlserver://localhost:1422;databaseName\=VIM_VCDB (user name, password, and database type to be passed separately)

- Connect to local server with integrated security:

  jdbc:sqlserver://localhost\\SQLEXP_VIM;databaseName=VIM_VCDB;integratedSecurity=true

- Connect to local server without integrated security:

  jdbc:sqlserver://localhost\\SQLEXP_VIM;databaseName\=VIM_VCDB (user name, password, and database type to be passed separately)

VMware vCenter Server JDBC configuration for Microsoft SQL Server might not work by default with direct IPv6 addresses. You must use one of the following forms:

- Use the host name form for a standard Type-4 JDBC URL (recommended):

  jdbc:sqlserver://*database-fully-qualified-host-name*:*port*

- Use direct IPv6 address format:

  jdbc:sqlserver://;serverName=[*IPv6-address*]

For more information about JDBC URL formatting for MS SQL databases, including port and instance configuration options, see the msdn.microsoft.com Web site. At the time of this topic's publication, the information was available at http://msdn.microsoft.com/en-us/library/ms378428.aspx.

JDBC URL Formats for Oracle Databases

For Oracle databases, you can use the following example JDBC URLs as a model:

- This format requires host name and address, port (default 1521) and service name (for example, "oracle.world"):

  jdbc:oracle:thin:@*host*:*port*/*service*

- This format requires host name and address, port (default 1521) and SID (for example, "ORCL"):

  jdbc:oracle:thin:@*host*:*port*:*SID*

- This format is for a fully configured Oracle client with Oracle Net, which is useful for non-TCP configuration or Oracle RAC (real application clusters):

  jdbc:oracle:thin:@*tnsname*

- The following example is for an Oracle RAC with a thin driver, without the full Oracle client installed:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=rac1-vip)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=rac2-vip)(PORT=1521))(LOAD_BALANCE=yes)(FAILOVER=ON)
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=RAC.DBTEAM)(FAILOVER_MODE=(BACKUP=rac1)
(TYPE=SELECT)(METHOD=BASIC)))))
```

In this example, **rac1-vip** is first node virtual IP, **rac2-vip** is second node virtual IP, **RAC.DBTEAM** is RAC DB service name, and **rac1** is name of failover node.

For more information about JDBC URL formatting for Oracle databases, see the oracle.com Web site. At the time of this topic's publication, the information was available at http://download.oracle.com/docs/cd/B28359_01/java.111/b31224/urls.htm/BEIJFHHB

JDBC URL Formats for IBM DB2 Databases

For IBM DB2 databases, you can use the following example JDBC URLs as a model:

- This format requires host name and address, port (for example, 50000) and database name (as created at the server):

  jdbc:db2://*host*:*port*/*database*

- This format is for a fully configured DB2 client (namely "IBM Data Server Client"), where ***database*** is the local database alias. This example is useful for non-TCP configurations:

  jdbc:db2:*database*

For more information about JDBC URL formatting for IBM DB2 databases, see the publib.boulder.ibm.com Web site.

Configure the URLs on a Standalone vCenter Server System

If you join a standalone vCenter Server system to a Linked Mode group, the domain name of the system must match the machine name. If you change either name to make them match, you must configure the vCenter Server URLs to make them compatible with the new domain name and machine name.

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

The vCenter Server installer configures default URL entries as follows:

- For the VirtualCenter.VimApiUrl key, the default value is `http(s)://`*`FQDN of VC machine`*`/sdk`.
- For the Virtualcenter.VimWebServicesUrl key, the default value is `https://`*`FQDN of VC machine`*`:`*`installed-webservices-port`*`/vws`.

Procedure

1. From the vSphere Client, connect directly to the vCenter Server instance on which you have changed the domain or host name.
2. Select **Administration > vCenter Server Settings**.
3. Click **Advanced Settings**.
4. For the VirtualCenter.VimApiUrl key, change the value to point to the location where the vSphere Client and SDK clients can access the vCenter Server system.

   For example: `http(s)://`*`machine-name/ip`*`:`*`vc-port`*`/sdk`.
5. For the VirtualCenter.VimWebServicesUrl key, change the value to point to the location where vCenter Server Webservices is installed.

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

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

Running the vCenter Server and vSphere Client Installers from a Network Drive

You can run the installers from a network drive, but you cannot install the software on a network drive.

In Windows, you can run the installers from the network drive and install the software on the local machine.

Required Information for Installing or Upgrading vCenter Single Sign-On, Inventory Service, and vCenter Server

Prepare for the vCenter Server installation by recording the values that the vCenter Server system requires.

The vCenter Server installation wizard prompts you for the installation information. Keep a record of the values entered, in case you must reinstall vCenter Server. You can print this topic as a worksheet to record the information that you need for the installation or upgrade.

NOTE Depending on the type of installation or upgrade you are doing, some entries might not be required.

Table 10-1. Information Required for vCenter Single Sign-On Installation

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
Single Sign-On deployment type. (Not applicable for Simple Install.) Create the primary node for a new vCenter Single Sign-On installation or an additional node to join to an existing high availability or multisite vCenter Single Sign-On installation.		
If you are creating the primary node for a new Single Sign-On installation, choose one of the following options. (Not applicable for Simple Install.) ■ Basic: the only node in a single node Single Sign-On installation, accessible by local system users. ■ The primary node for a new multinode high availability or multisite Single Sign-On installation.		
If you are creating an additional node to join to an existing high availability or multisite vCenter Single Sign-On installation, select one of the following options. (Not applicable for Simple Install.) ■ High availability: for scalability and availability. You can install multiple Single Sign-On servers and place them behind a load balancer. ■ Multisite: for large enterprises with multiple physical locations. Each physical site should have its own Single Sign-On cluster, to allow fast local Single Sign-On access.		

Table 10-1. Information Required for vCenter Single Sign-On Installation (Continued)

Required Information	Default	Your Entry
User name and password for the vCenter Single Sign-On administrator user account. You must use the same vCenter Single Sign-On user name and password name when you install vCenter Single Sign-On, and install or upgrade Inventory Service, vCenter Server, and the vSphere Web Client. IMPORTANT Be sure to record the password. If you need to restore the Single Sign-On configuration from a backup, the restore process requires the password you enter for the original Single Sign-On installation, even if you change the password later. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.	admin@System-Domain	You cannot change the user name from the default during installation.
RSA_DBA password and RSA_USER password (for the bundled Microsoft SQL Server 2008 R2 Express database). If you are using the bundled database, the Sign-On installer creates the RSA_DBA and RSA_USER users, which are used to set up the Single Sign-On database schema and to perform certain steps after the installation. You must enter passwords for these users. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.		
Database type (for an existing database). Supported version of Microsoft SQL, Oracle, or IBM DB2. See the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? for supported versions.		
Database name (for an existing database).		The name of the existing database you created for Single Sign-On. The name can contain only alphanumeric characters.
Host name or IP address (for an existing database). The Single Sign-On database requires a static host name or IP address.		
Oracle SID (optional, for an existing Oracle database)		
Port (for an existing database). The Single Sign-On database requires a static port.	Microsoft SQL: 1433 Oracle: 1521 DB2: 50000	
Service name (for an existing Oracle database)		
Database user name (for an existing database). Enter the database user name of a user who has the required permissions. See "Required vCenter Single Sign-On Database Users," on page 243.		
Database password (for an existing database).		
Database user name (for an existing database). Enter the database user name of a user who has the required permissions. For a list of required permissions, see "Required vCenter Single Sign-On Database Users," on page 243.		

Table 10-1. Information Required for vCenter Single Sign-On Installation (Continued)

Required Information	Default	Your Entry
Database DBA user name (for an existing database). Enter the database user name of a user who has the required permissions. For a list of required permissions, see "Required vCenter Single Sign-On Database Users," on page 243.		
Database DBA password (for an existing database).		
JDBC URL (optional, for an existing database). JDBC connection information required if you are using an existing vCenter Single Sign-On database. If you are entering the JDBC URL, see "JDBC URL Formats for the vCenter Server Database," on page 234		
vCenter Single Sign-On Fully Qualified Domain Name or IP address.	The fully qualified host name of the current machine	The DNS machine name you entered for your IP.
SSPI service account information You can use the default Windows NetworkService account, or enter the account information for an administrator user.		If you plan to create a high availability Single Sign-On deployment, change this to an Active Directory user.
Destination folder. The folder in which to install vCenter Single Sign-On. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).	`C:\Program Files\VMware\Infrastructure`	
vCenter Single Sign-On HTTPS port.	7444	

Table 10-2. Information Required for Inventory Service Installation or Upgrade

Required Information		Default	Your Entry
Setup Language. This selection controls the language only for the installer.		English	
Destination folder. The folder to install Inventory Service in. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).		`C:\Program Files\VMware\Infrastructure`	
Fully Qualified Domain Name. The FQDN for the Inventory Service local system.			
vCenter Inventory Service HTTPS port.	See "Required Ports for vCenter Server," on page 39.	10443	
vCenter Inventory Service management port.		10111	
vCenter Inventory Service Linked Mode communication port.		10109	

Table 10-2. Information Required for Inventory Service Installation or Upgrade (Continued)

Required Information	Default	Your Entry
Inventory size. The inventory size of your vCenter Server deployment: ■ Small (less than 100 hosts or 1000 virtual machines. ■ Medium (100-400 hosts or 1000-4000 virtual machines. ■ Large (more than 400 hosts or 4000 virtual machines. 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 "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.		
User name for the vCenter Single Sign-On administrator user account. You must use the same vCenter Single Sign-On user name and password name when you install vCenter Single Sign-On, and install or upgrade Inventory Service, vCenter Server, and the vSphere Web Client.	admin@System-Domain	
Lookup Service URL. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. If you enter a different port number when you install vCenter Single Sign-On, use that port number.		

Table 10-3. Information Required for vCenter Server Installation or Upgrade

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
vCenter Server license key. If you omit the license key, vCenter Server is installed in evaluation mode. After you install vCenter Server, you can enter the vCenter Server license in the vSphere Client.		
Data source name (DSN). Required if you use an existing database. Not required if you are using the bundled Microsoft SQL Server 2008 Express database. Leading and trailing spaces are not supported. Remove spaces from the beginning or end of the DSN.		
Database user name. Database password.	Required to use an existing database. Not required if you are using the bundled database. Non-ASCII characters are not supported.	
JDBC URL for database. Required if you use an existing database. The vCenter Server installer should generate and validate the JDBC URL for the vCenter Server database. If the installer fails to connect to the database by using the generated JDBC URL, the installer prompts you to specify the JDBC URL. The format of the JDBC URL depends on the database that you are using. See "JDBC URL Formats for the vCenter Server Database," on page 234.v		

Table 10-3. Information Required for vCenter Server Installation or Upgrade (Continued)

Required Information	Default	Your Entry
vCenter Server Service account information. Can be the Microsoft Windows system account or a user-specified account. Use a user-specified account if you plan to use Microsoft Windows authentication for SQL Server.	Microsoft Windows system account	
Fully qualified domain name (FQDN) for the vCenter Server machine The FQDN of the system that you are installing vCenter Server on. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message appears. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.		
Standalone or join group. Join a Linked Mode group to enable the vSphere Client to view, search, and manage data across multiple vCenter Server systems.	Standalone	
Fully qualified domain name of Directory Services for the vCenter Server group. The FQDN of a remote instance of vCenter Server. Required if this instance of vCenter Server is joining a group. The local and remote instances will be members of a Linked Mode group.		
LDAP port for the Directory Services for the remote vCenter Server instance. The LDAP port of the remote instance. Required if this instance of vCenter Server is joining a Linked Mode group. See "Required Ports for vCenter Server," on page 39.	389	
vCenter Server HTTPS port.	443	
vCenter Server HTTP port.	80	
Heartbeat port (UDP) used for sending data to ESX/ESXi hosts.	902	
VMware VirtualCenter Management Webservices.	8080	
VMware VirtualCenter Management Webservices.	8443	
Web Services change service notification port.	60099	
LDAP port for the Directory Services for the local vCenter Server instance.	389	
SSL port for the Directory Services for the local vCenter Server instance.	636	

See "Required Ports for vCenter Server," on page 39.

Table 10-3. Information Required for vCenter Server Installation or Upgrade (Continued)

Required Information		Default	Your Entry
Ephemeral ports. Select **Increase 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.			
Inventory size. The inventory size of your vCenter Server deployment: ■ Small (less than 100 hosts or 1000 virtual machines. ■ Medium (100-400 hosts or 1000-4000 virtual machines. ■ Large (more than 400 hosts or 4000 virtual machines. 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 "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.			
User name for the vCenter Single Sign-On administrator user account.	You must use the same vCenter Single Sign-On user name and password name when you install vCenter Single Sign-On, and install or upgrade Inventory Service, vCenter Server, and the vSphere Web Client.	admin@System-Domain	
Password for the vCenter Single Sign-On administrator user account.			
vCenter Server administrator recognized by vCenter Single Sign-On. The vCenter Server Administrator user or Users group who will have administrator privileges and can log in to vCenter Server after installation. You can also enter a domain user, in the form *user@domain_name* or a domain users group, in the form *domain_group@domain_name*.		If Single Sign-On is installed on the same host machine as vCenter Server: the local Administrators group. If Single Sign-On is installed on a different host machine than vCenter Server: admin@System-Domain.	
Lookup Service URL. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. If you enter a different port number when you install vCenter Single Sign-On, use that port number.			

Table 10-3. Information Required for vCenter Server Installation or Upgrade (Continued)

Required Information	Default	Your Entry
Inventory Service URL. The inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you enter a different port number when you install Inventory Service, use that port number.		
Destination folder. The folder to install vCenter Server in. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).	`C:\Program Files\VMware\Infrastructure`	

Required vCenter Single Sign-On Database Users

When you use an existing database rather than the database bundled with vCenter Single Sign-On, the installation process requires database users with certain permissions.

When you install Single Sign-On installation using an existing database, the installer requires you to enter the user names and passwords of an existing database administrator and a database user.

When you install Single Sign-On with the bundled Microsoft SQL Server 2008 R2 Express database, the installer creates two users:

- A database administrator user (for example, RSA_DBA) and password, which are used to set up the Single Sign-On database schema.
- A database user (for example, RSA_USER) and password, which are used to perform certain steps after the installation.

The installer prompts you to enter the passwords for these users.

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 the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Installing vCenter Server 11

After you install vCenter Server and the vSphere Client, you can configure communication between them.

This chapter includes the following topics:

vCenter Server Components and Support Tools

When you install vCenter Server, other components are also installed.

The following components can also be installed when you install vCenter Server.

VMware vCenter Server — Windows service to manage ESXi and legacy ESX hosts.

vCenter Single Sign On — The vCenter Single Sign On authentication service makes the VMware cloud infrastructure platform more secure by allowing the various vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. Available and required with vCenter Server 5.1.

vCenter Inventory Service — Inventory Service stores vCenter Server application and inventory data, enabling you to search and access inventory objects across linked vCenter Servers.

Microsoft .NET 3.5 SP1 Framework — Software used by the Database Upgrade wizard and the vSphere Client. Also used by vCenter Server if you are using the bundled database. If it is not installed on your system, the vCenter Server installer installs it.

Microsoft Windows Installer version 4.5	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 also install MSI 4.5 directly from the vCenter Server `autorun.exe` installer.
VMware vCenter Orchestrator	vCenter Server module that provides a set of tools to manage your virtual IT environment. vCenter Orchestrator module is not supported on IPv6-only operating systems. If you install vCenter Server in a mixed environment (both IPv4 and IPv6 enabled), the vCenter Orchestrator module can be configured using IPv4. See the *Administering vCenter Orchestrator*. This component is installed automatically with vCenter Server.
Microsoft SQL Server 2008 R2 Express (optional)	Free, bundled version of the Microsoft SQL Server database for smaller scale applications. If you choose to use an existing database, the installer does not install the bundled database.
vSphere Client	Client application used to connect to an ESXi or legacy ESX host directly, or indirectly through a vCenter Server.
vSphere Web Client	Server application that provides a browser-based alternative to the vSphere Client. You can use the vSphere Web Client to manage an ESXi host by Web browser through a vCenter Server.
vSphere Update Manager	vCenter Server component that provides security monitoring and patching support for hosts and virtual machines.
vSphere ESXi Dump Collector	vCenter Server support tool. You can configure ESXi to dump the vmkernel memory to a network server, rather than to a disk, when the system has encountered a critical failure. The Dump Collector collects such memory dumps over the network.
vSphere Syslog Collector	vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.
vSphere Auto Deploy	vCenter Server support tool that can provision hundreds of physical hosts with ESXi software. You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts, and a vCenter Server location (folder or cluster) for each host.
vSphere Authentication Proxy	vCenter Server support tool that enables ESXi hosts to join a domain without using Active Directory credentials. This tool enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy, by removing the need to store Active Directory credentials in the host configuration.

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.

Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install

You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments.

Alternatively, you can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components. See "Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server," on page 251.

If vCenter Inventory Service and vCenter Server are installed on the computer, this procedure upgrades vCenter Inventory Service and vCenter Server.

Prerequisites

- Review "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

1 Install vCenter Single Sign-On as Part of a vCenter Server Simple Install on page 247

   Create the only node in a basic vCenter Single Sign-On installation.

2 Install or Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install on page 248

   You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments.

3 Install vCenter Server as Part of a Simple Install on page 249

   You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments.

Install vCenter Single Sign-On as Part of a vCenter Server Simple Install

Create the only node in a basic vCenter Single Sign-On installation.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224 and the *vSphere Security* documentation.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See the first topic in this multitopic task: "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221

Procedure

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

2 Select **VMware® vCenter™ Simple Install**, and click **Install**.

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

4 Set the password for the vCenter Single Sign-On administrator account.

The password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character.

5 Select the database type for vCenter Single Sign-On.

6 If you are using an existing database, to ensure that table space is created for the database, run the script `rsaIMSLite<DBName>SetupTablespaces.sql`. The script is located at *`vCenter Server Installation directory`*`\Single Sign On\DBScripts\SSOServer\Schema\`*`your_existing_database`*.

You can leave the installer to run the script, and resume the installer from this panel.

7 If you are using the bundled Microsoft SQL Server 2008 R2 Express database, enter the passwords for a Single Sign-On database administrator and database user. The installer uses these credentials to create the users in the database.

The password must comply with Windows Group Policy Object (GPO) password policies for your local operating system and AD domain. The password must be 32 characters or less. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.

8 If you are using an existing database, enter the JDBC connection information.

9 Enter the FQDN or IP address for the vCenter Single Sign-On host machine.

10 (Optional) Enter the SSPI service account information.

You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.

11 Select the folder in which to install vCenter Single Sign-On.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

12 Accept or change the HTTPS port for vCenter Single Sign-On.

13 Click **Install.**

vCenter Single Sign-On is installed, and the vCenter Inventory Service installation or upgrade wizard starts.

What to do next

Install or upgrade vCenter Inventory Service. See "Install or Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install," on page 248.

Install or Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install

You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments.

This task continues the vCenter Server Simple Install from the task "Install vCenter Single Sign-On as Part of a vCenter Server Simple Install," on page 247.

If Inventory Service is installed on the computer, this procedure upgrades Inventory Service.

Prerequisites

- See the first topic in this multitopic task: "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

1 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

2 Click **Install**.

Inventory Service is installed, and the vCenter Server installation wizard starts.

What to do next

Install vCenter Server. Proceed to "Install vCenter Server as Part of a Simple Install," on page 249.

Install vCenter Server as Part of a Simple Install

You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments.

This task continues the vCenter Server Simple Install from the task "Install or Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install," on page 248

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See the first topic in this multitopic task: "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221

Procedure

1 (Optional) Enter your license key.

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

2 Choose the type of database that you want to use.

- To use the bundled database, click **Install a Microsoft SQL Server 2008 Express instance (for small-scale deployments)**.

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

- To use an existing database, click **Use an existing supported database** and select your database from the list of available DSNs. Enter the user name and password for the DSN.

If your database uses Windows NT authentication, the user name and password fields are disabled.

NOTE A warning might appear that the DSN points to an older version of a repository that must be upgraded. If you click **Yes**, the installer upgrades the database schema, making the database irreversibly incompatible with previous VirtualCenter versions. See the *vSphere Upgrade* documentation.

3 Set the vCenter Server service account information.

- To use the bundled database, click **Install a Microsoft SQL Server 2008 Express instance (for small-scale deployments: up to 5 hosts and 50 virtual machines)**.
- If you are using a nonbundled database, enter the administrator name and password that you use when you log in to the system on which you are installing vCenter Server.
- If you are using the bundled SQL Server database, select **Use SYSTEM Account**.

You need the user name and password entered here to log in to vCenter Server after you have installed it.

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

4 For each component that you install, accept the default port numbers, or if another service is using the defaults, enter alternative ports.

5 (Optional) Select **Increase the number of available ephemeral ports**.

6 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 topic vCenter Server Hardware Requirements.

7 Click **Install**.

Multiple progress bars appear during the installation of the selected components.

The vCenter Simple Install is complete.

What to do next

After you install vCenter Server, you can display the vCenter Server welcome page by typing the IP address of the vCenter Server machine or by typing `localhost` from a browser installed on the vCenter Server machine. From the welcome page, you can download the vSphere Client, or log in to the vSphere Web Client, after the vSphere Web Client is installed and the vCenter Server is registered. You can also access vSphere documentation.

See Chapter 12, "After You Install vCenter Server," on page 279.

Back up the vCenter Single Sign On configuration and database. See "Back Up the vCenter Single Sign On Configuration," on page 291.

Back up the Inventory Service database. See "Back Up the Inventory Service Database on Windows," on page 302.

Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server

You can install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

Alternatively, you can install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

Prerequisites

- Review "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

1 Separately Install vCenter Single Sign-On on page 251

   You can install vCenter Single Sign-On in a basic, high availability, or multisite deployment.

2 Install or Upgrade the vSphere Web Client on page 264

   The vSphere Web Client lets you connect to a vCenter Server system to manage an ESXi host through a browser.

3 Confirm Active Directory Domains for vCenter Server Administrators on page 265

   After you install vCenter Single Sign-On, confirm that any vCenter Server administrators in existing Active Directory (AD) domains are recognized by Single Sign-On.

4 Install or Upgrade vCenter Inventory Service in a Separate Installation on page 266

   You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

5 (Optional) Replicate Data Between Multisite Single Sign-On Instances in a New vCenter Server Deployment on page 267

   Automatic replication of data between Single Sign-On sites is not supported in a multisite deployment. After you install or make a change to one of the Single Sign-On instances, you must perform a manual data export and import operation with a command-line tool.

6 Install vCenter Server in a Separate Installation on page 268

   You can install vCenter Server separately from vCenter Single Sign-On and vCenter Inventory Service to customize the location and configuration of the components.

Separately Install vCenter Single Sign-On

You can install vCenter Single Sign-On in a basic, high availability, or multisite deployment.

To understand the Single Sign-On basic, high availability, and multisite deployment options, see "vCenter Single Sign-On Deployment Modes," on page 225.

Alternatively, you can install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. This option is appropriate for small deployments. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

Prerequisites

- Review "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

- Review "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224.

Procedure

- Choose one of the following vCenter Single Sign-On deployments.
  - "Separately Install vCenter Single Sign-On in a Basic Deployment," on page 252.
  - "Install and Configure vCenter Single Sign-On for a High Availability Deployment," on page 253.
  - "Install and Configure vCenter Single Sign-On for a Multisite Deployment," on page 260.

Separately Install vCenter Single Sign-On in a Basic Deployment

Create the only node in a basic vCenter Single Sign-On installation.

Before you install Single Sign-On in basic mode, consider carefully the future requirements for the deployment to determine whether a multisite or high availability deployment is appropriate. If you install a Single Sign-On instance in basic mode, you cannot later promote the instance to a high availability or multisite node.

To install vCenter Single Sign-On in high availability mode, see "Install and Configure vCenter Single Sign-On for a High Availability Deployment," on page 253. To install vCenter Single Sign-On in multisite mode, see "Install and Configure vCenter Single Sign-On for a Multisite Deployment," on page 260.

These instructions let you install vCenter Single Sign-On only. You must install vCenter Single Sign-On and Inventory Service before installing vCenter Server. For simple deployments, you can install vCenter Single Sign-On, Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224 and the *vSphere Security* documentation.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See the first topic in this multitopic task: "Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server," on page 251.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221
- Review "vCenter Single Sign-On Deployment Modes," on page 225.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter™Single Sign On** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Select **Create the primary node for a new Single Sign On installation**.
5. Select **Install basic vCenter Single Sign On**.
6. Set the password for the vCenter Single Sign-On administrator account.

   The password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character.

7 Select the database type for vCenter Single Sign-On.

8 If you are using an existing database, to ensure that table space is created for the database, run the script `rsaIMSLite<DBName>SetupTablespaces.sql`. The script is located at *`vCenter Server Installation directory`*`\Single Sign On\DBScripts\SSOServer\Schema\`*`your_existing_database`*.

   You can leave the installer to run the script, and resume the installer from this panel.

9 If you are using an existing database for Single Sign On, and you have not already done so, create a database user (RSA_USER) and database administrator (RSA_DBA), by running the script `rsaIMSLite`*`DBName`*`SetupUsers.sql`. The script is included in the vCenter Server installer download package, at *`vCenter Server Installation directory`*`\SSOServer`.

   You can leave the installer to run the script, and resume the installer from this panel.

10 If you are using the bundled Microsoft SQL Server 2008 R2 Express database, enter the passwords for a Single Sign-On database administrator and database user. The installer uses these credentials to create the users in the database.

   The password must comply with Windows Group Policy Object (GPO) password policies for your local operating system and AD domain. The password must be 32 characters or less. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.

11 If you are using an existing database, enter the JDBC connection information.

12 Enter the FQDN or IP address for the vCenter Single Sign-On host machine.

13 (Optional) Enter the SSPI service account information.

   You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.

14 Select the folder in which to install vCenter Single Sign-On.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

15 Accept or change the HTTPS port for vCenter Single Sign-On.

16 Click **Install.**

vCenter Single Sign-On is installed.

What to do next

Back up the vCenter Single Sign-On configuration and database. See "Back Up the vCenter Single Sign On Configuration," on page 291.

Install Inventory Service. See "Install or Upgrade vCenter Inventory Service in a Separate Installation," on page 266.

Install and Configure vCenter Single Sign-On for a High Availability Deployment

In high availability mode, two nodes work with the same database, data, and user stores to ensure that vCenter Single Sign-On is not a single point of failure.

NOTE When configured for high availability, vCenter Single Sign-On cannot cannot authenticate local OS Windows users. However, it can authenticate Active Domain users.

Prerequisites

- Review Prerequisites for Installing vCenter Single Sign On, vCenter Inventory Service, and vCenter Server.

Procedure

1 Prepare Virtual or Physical Machines for vCenter Single Sign-On High Availability on page 254

Configuring vCenter Single Sign-On for high availability requires two machines. One machine acts as the primary node, and the other as the backup node. When configured for high availability, both nodes work with the same database, use the same data, and have the same user stores

2 Install the First Node in a High Availability Installation on page 255

Create the first node in a vCenter Single Sign-On installation for high availability.

3 Install an Additional Node in an Existing High Availability vCenter Server Single Sign-On Installation on page 255

Create an additional vCenter Single Sign-On node for an existing high availability vCenter Single Sign-On installation.

4 Configure the Load Balancing Software on page 256

You can configure any SSL-aware load balancer (physical or virtual) to act as load balancing software with Single Sign-On, increasing availability.

5 Configure Single Sign-On Load Balancing on page 257

Configure the load balancing software. Because Single Sign-On sends and receives sensitive information, configure the load balancing software for SSL.

6 Update the Lookup Service Records on page 258

When you configure Single Sign-On for high availability, update the Lookup Service records to ensure that the load balancer can connect to the Single Sign-On nodes.

Prepare Virtual or Physical Machines for vCenter Single Sign-On High Availability

Configuring vCenter Single Sign-On for high availability requires two machines. One machine acts as the primary node, and the other as the backup node. When configured for high availability, both nodes work with the same database, use the same data, and have the same user stores

Procedure

1 Obtain or create two virtual machines.

- Create two virtual machines running a Windows guest operating system.
- Obtain two physical machines running a Windows operating system.

2 Create a DNS entry for each virtual machine.

3 (Optional) If you use Active Directory and want vCenter Single Sign-On to discover it automatically, do the following tasks.

- Put both machines in the same Active Directory domain.
- Assign administrative permissions on both machines to the Active Directory domain user with which you run the installation.

The machines are ready to become vCenter Single Sign-On nodes.

What to do next

Install vCenter Single Sign-On to create the nodes.

Install the First Node in a High Availability Installation

Create the first node in a vCenter Single Sign-On installation for high availability.

Note vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224 and the *vSphere Security* documentation.

Prerequisites

- Review Prerequisites for Installing vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter™Single Sign-On** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Select **Create the primary node for a new Single Sign-On installation**.
5. Select the Single Sign-On type, **Create the primary node for a new Single Sign-On installation**.
6. Set the password for the vCenter Single Sign-On administrator account.
7. Select the database type for vCenter Single Sign-On.
8. Select the database type for vCenter Single Sign-On.
   a. If you are using the bundled Microsoft SQL Server 2008 R2 Express database, enter the passwords for a Single Sign-On database administrator and database user. The installer uses these credentials to create the users in the database.
   b. If you are using an existing database, enter the JDBC connection information.
9. Enter the FQDN or IP address for the vCenter Single Sign-On host machine.
10. (Optional) Enter the SSPI service account information.

    You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.
11. Select the folder in which to install vCenter Single Sign-On.
12. Accept or change the HTTPS port for vCenter Single Sign-On.
13. Click **Install.**

Install an Additional Node in an Existing High Availability vCenter Server Single Sign-On Installation

Create an additional vCenter Single Sign-On node for an existing high availability vCenter Single Sign-On installation.

To create the only node in a basic vCenter Single Sign-On installation, see "Separately Install vCenter Single Sign-On in a Basic Deployment," on page 252.

If you are installing Single Sign-On on a multisite installation, see "Install an Additional Node for a Multisite vCenter Single Sign-On Installation," on page 262

Prerequisites

See the previous steps in this multitask topic, "Install and Configure vCenter Single Sign-On for a High Availability Deployment," on page 253

Procedure

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

2 In the Single Sign On Deployment Type panel, select **Join an existing Single Sign On installation**.

3 Select the Single Sign-On type, and enter the connection information for the existing primary node of the Single Sign-On installation that you are adding this node to.

By default, the Single Sign-On port is 7444. If you assigned a different port when you installed Single Sign-On, use that port.

4 Click **Install**.

What to do next

Continue to the next task, "Configure the Load Balancing Software," on page 256.

Configure the Load Balancing Software

You can configure any SSL-aware load balancer (physical or virtual) to act as load balancing software with Single Sign-On, increasing availability.

You define four paths in the load balancer configuration, one for each Single Sign-On interface: STS, Group Check, Lookup Service (all high availability nodes), and the SSO Admin SDK (primary node only). Sensitive information such as passwords are passed to and from vCenter Single Sign-On. Configure the Apache HTTPD software for SSL and use only SSL ports as proxies to the Single Sign-On server.

Prerequisites

NOTE This is provided as an example of configuring your load balancing software using Apache HTTPD. Other load balancers will be configured in a different way.

Verify that you have two Single Sign-On nodes and Apache HTTPD set up as a load balancer. For information about setting up your load balancing software, see KB article 2034157.

Procedure

- Define the paths, configure the proxy-related and load balancer-related directives.

  Add the VirtualHost entry at the end of the `httpd-ssl.conf` file, or you can update an existing VirtualHost entry.

  NOTE You might encounter errors using 64-bit Microsoft Windows operating systems. Update the following value in the `conf/extra/httpd-ssl.conf file`: `SSLSessionCache "shmcb:C:/PROGRA\~2/Apache Software Foundation/Apache2.2/logs/ssl_scache (5120000)`

What to do next

"Update the HTTPD Configuration with SSL Certificates," on page 257.

Update the HTTPD Configuration with SSL Certificates

Continuing with the Apache HTTPD load balancer example, after configuring the Apache HTTPD server, configure HTTPD to use SSL certificates.

Prerequisites

NOTE This example describes using Apache HTTPD as your load balancer. Other load balancers will be configured differently.

Verify that you have the custom certificates.

Procedure

1 In a text editor, locate and open `conf/extra/httpd-ssl.conf`.

2 Type the location of your SSL server certificate.

```
SSLCertificateFile "C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/conf/certs/server.crt"
```

3 Type the SSL server private key for your custom load balancer certificate.

```
SSLCertificateKeyFile "C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/conf/certs/server.key"
```

4 Type the file that contains the entire certificate chain (or if you have only the leaf and root, you can provide the CA).

```
SSLCertificateChainFile "C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/conf/certs/ca/cacert.pem"
```

5 To ensure that clients can authenticate to the server, type the following directive.

```
SSLVerifyClient none
```

6 Restart the Apache server.

What to do next

Update the LookUp Service records.

Configure Single Sign-On Load Balancing

Configure the load balancing software. Because Single Sign-On sends and receives sensitive information, configure the load balancing software for SSL.

Prerequisites

- You must have created both a primary and a backup Single Sign-On node.
- You must have a supported load balancing software program installed.

Procedure

1 Configure node affinity for the machine on which the primary node is installed.

2 Add entries for the following Single Sign-On services.

Table 11-1. Service Entries

Service	Map	On node
Groupcheck	`/groupcheck` to `/sso-adminserver`	both
LookupService	`/lookupservice`	both

Table 11-1. Service Entries (Continued)

Service	Map	On node
Security Token Service	`/ims`	both
Admin server	`/sso-adminserver` to `/sso-adminserver`	primary only

NOTE Because Groupcheck is present on both of the nodes but Admin server is only present on the primary node, do not use the same path for Groupcheck and Admin server.

What to do next

"Update the Lookup Service Records," on page 258

Update the Lookup Service Records

When you configure Single Sign-On for high availability, update the Lookup Service records to ensure that the load balancer can connect to the Single Sign-On nodes.

Procedure

1 Copy the root certificate of the certificate chain that issued the SSL certificate for the load balancing software to the machine on which Single Sign-On `node1` (the primary node) is installed.

2 From a terminal window, on each of the systems where Single Sign-On is installed, perform the following steps.

   a Set the *JAVA_HOME* variable.

   By default, VMware products install JRE in `C:\Program Files\VMware\Infrastructure\jre`.

   b Check your firewall settings to ensure that connections to the load balancing software are possible.

   c List the services in the directory where you installed Single Sign-On.

   If you installed the software in the default location, run the following command to change to the directory.

   ```
   cd /d C:\Program Files\VMware\Infrastructure\SSOServer\ssolscli
   ```

   Get the list of services.

   ```
   ssolscli listServices https://primary_node_hostname:7444/lookupservice/sdk
   ```

3 From the list of services, locate the `Group Check`, `SSO Admin`, and `Security Token Service (STS)` services and determine the `Type`.

Table 11-2. Service type

Type	URN
Groupcheck	urn:sso:groupcheck
Admin	urn:sso:admin
Security Token Service	urn:sso:sts

4 Create a properties file for each service, naming the files `gc.properties`, `admin.properties`, and `sts.properties`, respectively.

The URIs specified for the Single Sign-On Admin and Group Check are the ones that you specified in the load balancing software configuration.

An example `.properties` file looks similar to this one.

```
[service]
friendlyName=STS for Single Sign On
version=1.0
ownerId=
type=urn:sso:sts
description=Security Token Service of Single Sign On server

[endpoint0]
uri=https://location_of_your_load_balancer:configured port/ims/STSService?wsdl
ssl=C:\location_of_pem\cacert.pem
protocol=wsTrust
```

5 Locate the serviceId for each of the three services.

The service ID is located in serviceId on the list of services you created.

6 Using a plain text editor, create a service ID file for each service.

Table 11-3. File names

Service	File name
sts.properties	`sts_id`
gc.properties	`gc_id`
admin.properties	`admin_id`

The service ID file contains only the service ID and must not contain any other data.

The following is an example of the contents of the `sts_id` file.

```
{D46D4BFD-CC5B-4AE7-87DC-5CD63A97B194}:7
```

7 For each service, run the following commands.

```
SingleSignOn install dir\ssolscli\ssolscli updateService
 -d Lookup Service URL -u sso administrator name -p
sso administrator password -si serviceid_file
-ip service.properties
```

The following code is an example of the contents of the `sts_id` file.

```
C:\Program Files\VMware\Infrastructure\SSOServer\ssolscli\ssolscli
updateService -d https://primary_sso_node configured_port/
lookupservice/sdk -u admin@System-Domain -p VMware123
-si sts_id -ip sts.properties
```

What to do next

Install Inventory Service. See "Install or Upgrade vCenter Inventory Service in a Separate Installation," on page 266.

Note During the installation of vCenter Server, vSphere Web Client, and the Inventory service, you must provide the address of the new load balanced hostname for Lookup Service. The address should be in the form https://*load balancer fqdn*:*configured port*/*configured path*.

Install and Configure vCenter Single Sign-On for a Multisite Deployment

The vCenter Single Sign-On multisite configuration is designed for deployments with multiple physical locations. Installing a Single Sign-On instance at each site allows fast access to local authentication-related services. Each Single Sign-On instance is connected to the local instances of the AD (LDAP) servers and has its own database with local users and groups.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign On Affects vCenter Server Installation and Upgrades," on page 224 and the *vSphere Security* documentation.

For more information about multisite deployment mode, see "vCenter Single Sign-On Deployment Modes," on page 225.

To install vCenter Single Sign-On in high availability mode, see "Install and Configure vCenter Single Sign-On for a High Availability Deployment," on page 253. To install vCenter Single Sign-On in basic mode, see "Separately Install vCenter Single Sign-On in a Basic Deployment," on page 252.

These instructions let you install vCenter Single Sign-On only. You must install vCenter Single Sign-On and Inventory Service before installing vCenter Server. For simple deployments, you can install vCenter Single Sign-On, Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

After you install Single Sign-On, no connectivity between the Single Sign-On servers is necessary, because there is no automatic replication of data between Single Sign-On instances.

There are no components in the vSphere suite that communicate with multiple Single Sign-On servers. Each vSphere component should be configured to communicate with its local Single Sign-On instance for faster access.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

1 Install the First Node in a Multisite vCenter Single Sign-On Installation on page 260

   Create the first vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation.

2 Install an Additional Node for a Multisite vCenter Single Sign-On Installation on page 262

   Create an additional vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation.

Install the First Node in a Multisite vCenter Single Sign-On Installation

Create the first vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation.

Prerequisites

- Review "Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server," on page 251.
- Review "vCenter Single Sign-On Deployment Modes," on page 225.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221

Procedure

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

2 Select **vCenter™Single Sign On** and click **Install**.

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

4 In the vCenter Single Sign On Deployment Type wizard panel, select **Create the primary node for a new Single Sign On installation**.

5 In the panel that asks you to select single node type, select **Create the primary node for a new Single Sign On installation**.

6 Set the password for the vCenter Single Sign-On administrator account.

The password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character.

7 Select the database type for vCenter Single Sign-On.

8 If you are using an existing database, to ensure that table space is created for the database, run the script `rsaIMSLite<DBName>SetupTablespaces.sql`. The script is located at *`vCenter Server Installation directory`*`\Single Sign On\DBScripts\SSOServer\Schema\`*`your_existing_database`*.

You can leave the installer to run the script, and resume the installer from this panel.

9 If you are using an existing database for Single Sign On, and you have not already done so, create a database user (RSA_USER) and database administrator (RSA_DBA), by running the script `rsaIMSLite`*`DBName`*`SetupUsers.sql`. The script is included in the vCenter Server installer download package, at *`vCenter Server Installation directory`*`\SSOServer`.

You can leave the installer to run the script, and resume the installer from this panel.

10 If you are using the bundled Microsoft SQL Server 2008 R2 Express database, enter the passwords for a Single Sign-On database administrator and database user. The installer uses these credentials to create the users in the database.

The password must comply with Windows Group Policy Object (GPO) password policies for your local operating system and AD domain. The password must be 32 characters or less. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.

11 If you are using an existing database, enter the JDBC connection information.

12 Enter the FQDN or IP address for the vCenter Single Sign-On host machine.

13 (Optional) Enter the SSPI service account information.

You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.

14 Select the folder in which to install vCenter Single Sign-On.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

15 Accept or change the HTTPS port for vCenter Single Sign-On.

16 Click **Install.**

The first Single Sign-On multisite node is installed.

Install an Additional Node for a Multisite vCenter Single Sign-On Installation

Create an additional vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation.

Prerequisites

- Install the first node in the multisite vCenter Single Sign-On installation. See "Install the First Node in a Multisite vCenter Single Sign-On Installation," on page 260.
- Review "vCenter Single Sign-On Deployment Modes," on page 225.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

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

2 Select **vCenter™Single Sign On** and click **Install**.

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

4 In the Single Sign On Deployment Type panel, select **Join an existing Single Sign On installation**.

5 Select **Multisite**.

6 Enter the information to point this additional node to the primary Single Sign-On node.

NOTE If the primary node is a high-availability cluster, enter the address of the primatry node load balancer.

   a Enter the FQDN or IP address of the primary node.

   b Enter the HTTPS port of the primary node.

   c Enter the password for the vCenter Single Sign-On administrator account of the primary node: **`admin@System-Domain`**.

7 Set the password for the vCenter Single Sign-On administrator account.

   The password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character.

8 Select the database type for vCenter Single Sign-On.

9 If you are using an existing database, to ensure that table space is created for the database, run the script `rsaIMSLite<DBName>SetupTablespaces.sql`. The script is located at *`vCenter Server Installation directory`*`\Single Sign On\DBScripts\SSOServer\Schema\`*`your_existing_database`*.

   You can leave the installer to run the script, and resume the installer from this panel.

10 If you are using the bundled Microsoft SQL Server 2008 R2 Express database, enter the passwords for a Single Sign-On database administrator and database user. The installer uses these credentials to create the users in the database.

   The password must comply with Windows Group Policy Object (GPO) password policies for your local operating system and AD domain. The password must be 32 characters or less. The following characters are not supported in passwords: semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\). Passwords must comply with Windows Group Policy Object (GPO) password policy.

11 If you are using an existing database, enter the JDBC connection information.

12 Enter the FQDN or IP address for the vCenter Single Sign-On host machine.

13 (Optional) Enter the SSPI service account information.

You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.

14 Select the folder in which to install vCenter Single Sign-On.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

15 Accept or change the HTTPS port for vCenter Single Sign-On.

16 Click **Install.**

17 Select the Single Sign-On type, and enter the connection information for the existing primary node of the Single Sign-On installation that you are adding this node to.

By default, the Single Sign-On port is 7444. If you assigned a different port when you installed Single Sign-On, use that port.

18 Set the password for the vCenter Single Sign-On administrator account.

The password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character.

19 Select the database type for vCenter Single Sign-On.

20 If you are using an existing database, enter the credentials of a Single Sign-On database administrator with the appropriate permissions (for example, MSSQL database administrators require DBO and SYSADMIN permissions). The installer uses these credentials to create the users RSA_DBA and RSA_USER.

21 If you are using an existing database, enter the JDBC connection information.

22 Enter the FQDN or IP address for the vCenter Single Sign-On host machine.

23 (Optional) Enter the SSPI service account information.

You can use the default Windows NetworkService account, or enter the account information for an administrator user. This step applies only if you logged in as a domain account user to install Single Sign-On.

24 Select the folder in which to install vCenter Single Sign-On.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

25 Accept or change the HTTPS port for vCenter Single Sign-On.

26 Click **Install.**

The additional vCenter Single Sign-On Node is installed.

What to do next

Repeat this procedure for each additional multisite node.

NOTE After you install Single Sign-On and Inventory Service at each of the multisite nodes, replicate the Single Sign-On data between the nodes. See "(Optional) Replicate Data Between Multisite Single Sign-On Instances in a New vCenter Server Deployment," on page 267.

Install Inventory Service. See "Install or Upgrade vCenter Inventory Service in a Separate Installation," on page 266.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage an ESXi host through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client to version 5.1.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Client and vSphere Web Client Software Requirements," on page 38.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 232.
- Install vCenter Single Sign On, and install or upgrade Inventory Service and vCenter Server to version 5.1.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.
- If you are upgrading the vSphere Web Client, and you plan to use it with any version 5.0.x vCenter Server instance that was registered to a version 5.0 vSphere Web Client without accepting the SSL thumbprint, see "Version 5.1 vSphere Web Client Fails to Connect to Version 5.0.x vCenter Server," on page 283.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **VMware vSphere® Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Accept or change the default port settings.

5 Enter the information to register the vSphere Web Client with vCenter Single Sign On.

The vCenter Single Sign On administrator user name is admin@System-Domain, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign On. If you entered a different port number when you installed vCenter Single Sign On, use that port number.

NOTE If you installed vCenter Single Sign On in a vCenter Server Appliance, you can enter the Single Sign On Admin user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

---

6 Click **Install**.

7 Start the vSphere Web Client by doing one of the following actions.

- In a browser, go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- From the Windows Start menu, select **Programs > VMWare > VMware vSphere Web Client > vSphere Web Client**.

What to do next

Install the Client Integration Plug-In in the vSphere Web Client. See "Install the Client Integration Plug-In in the vSphere Web Client," on page 284

If you will use the vSphere Web Client with version 5.0.x vCenter Servers, register those vCenter Servers on the vSphere Web Client Administration Application page in the browser. You do not need to register version 5.1 vCenter Server systems that use the same vCenter Single Sign On server as the vSphere Web Client. The vSphere Web Client can locate such vCenter Server systems by using VMware Lookup Service. For instructions about registering a vCenter Server System with the vSphere Web Client, see the *vCenter Server and Host Management* documentation. If the browser fails to open or to display the Administration Application page correctly, open the application from the Windows **Start** menu: **Programs > VMware > VMware vSphere Web Client > vSphere Administration Application**

Confirm Active Directory Domains for vCenter Server Administrators

After you install vCenter Single Sign-On, confirm that any vCenter Server administrators in existing Active Directory (AD) domains are recognized by Single Sign-On.

If your administrators are AD users, they are migrated to Single Sign-On during a Single Sign On installation or upgrade, provided that Single Sign-On can find the AD domains. In the following circumstances, your local operating system users are not migrated to the new environment, and you will have to create new administrative users:

- Single Sign-On is deployed on a different machine from vCenter Server.
- Single Sign-On is deployed as a primary node in a high availability or multisite installation.

Prerequisites

- Install vCenter Single Sign-On.
- Install or upgrade the vSphere Web Client to the current version.

Procedure

1 Log in to the vSphere Web Client as the Single Sign-On administrator: **`admin@system-domain`**.

2 Make sure that you can access all the AD domains containing your vCenter Server administrators.

3 If you cannot access an AD domain, correct the problem and use the vSphere Web Client to add the AD domain.

See "If Autodiscovery Fails During Single Sign-On Installation Manually Add Active Directory Domains," on page 272 and VMware Knowledge Base article http://kb.vmware.com/kb/2035934.

4 Assign one of the AD users as a Single Sign-On administrator.

5 Log out of the vSphere Web Client and log back in as the new Single Sign-On administrator user.

If you are able to connect successfully, you have configured Single Sign-On correctly.

Install or Upgrade vCenter Inventory Service in a Separate Installation

You can install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions install vCenter Inventory Service only. You must install vCenter Single Sign On before installing Inventory Service and vCenter Server. For simple deployments, you can install vCenter Server, vCenter Single Sign On, and Inventory Service together on a single host machine using the vCenter Server Simple Install option. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

If vCenter Inventory Service is already installed on the computer, this procedure upgrades Inventory Service.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See the first topic in this multitopic task: "Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server," on page 251.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

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

2 Select **VMware® vCenter™ Inventory Service** and click **Install.**

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

4 Accept or change the default installation folder.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

5 Enter the fully qualified domain name for the Inventory Service host machine.

6 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

7 Accept or change the default values for Inventory Service port numbers.

8 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 topic vCenter Server Hardware Requirements.

9 Enter the information to register Inventory Service with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is admin@System-Domain, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

10 Click **Install Certificates**.

11 Click **Install**.

Inventory Service is installed.

What to do next

Install vCenter Server. See "Install vCenter Server in a Separate Installation," on page 268.

(Optional) Replicate Data Between Multisite Single Sign-On Instances in a New vCenter Server Deployment

Automatic replication of data between Single Sign-On sites is not supported in a multisite deployment. After you install or make a change to one of the Single Sign-On instances, you must perform a manual data export and import operation with a command-line tool.

The data to replicate includes local users and groups and the configuration of the STS server. Because this data rarely changes, you can schedule replications once a day or week, as appropriate. For specific instructions about manually replicating data between servers in a multisite Single Sign-On deployment, see the *vSphere Security* documentation.

These steps represent an accumulative change replication. Changes to one node are transported only to the node where the next changes will occur. After the last planned change is done, changes have been propagated to all nodes.

Alternatively, you can execute the replication sequentially. After a change in one node occurs, replicate it to all other nodes before making a change on any other node. During setup of the virtual infrastructure on each site, the better practice is to use the accumulative approach, which needs fewer steps, as the changes are planned and executed in a relatively short time span. For regular, ongoing operations, use the sequential approach.

CAUTION To ensure that data remains in sync during the manual replication process, do not make any changes to the data to be replicated, for example adding or deleting identity sources or local users.

This procedure completely overrides the state of the target node. You must perform manual transport of replication data sequentially. This means that changes on a node are propagated to all other nodes in the deployment before changes occur on any other nodes.

Prerequisites

- Verify that you have vCenter Single Sign-On administrator privileges on the vCenter Single Sign-On systems where you export or import the replication data.
- Install vCenter Single Sign-On and vCenter Inventory Service for each site in the multisite configuration before vCenter Server is installed.

Procedure

1 Install vCenter Server in the first site.

2 Export the Single Sign-On data from the first site and copy it to the second site.

3 Import the Single Sign-On data to the second site.

   a Log in to the vCenter Single Sign-On system where you will apply the change.

   b Navigate to the directory *SSO install directory*`sso-replication-cli`

   c Run `repl_tool.cmd` with the following parameters to import the replication state file.

   `import -f` *`file`* `-u` *`admin_user_name`* `[-p` *`password`*`]`

   Enter the following command-line parameters in the order listed.

Parameter	Value
mode	Import.
file	Relative or absolute path to a file from which the data is imported.
admin_user_name	Name of a valid vCenter Single Sign-On administrator user.
password	Optional. If you do not enter the password, you are prompted for a password when you run the command.

4 Install vCenter Server in the second site.

5 Following the procedure in steps Step 2 and Step 3, export the single Sign-On data from the second site and import it to the third site

6 Repeat the procedures in steps Step 4 and Step 5 for each succeeding site in the multisite configuration.

Single Sign-On data has been propagated to all nodes.

Install vCenter Server in a Separate Installation

You can install vCenter Server separately from vCenter Single Sign-On and vCenter Inventory Service to customize the location and configuration of the components.

These instructions let you install vCenter Server only. Alternatively, you can install vCenter Server, vCenter Single Sign-On, and Inventory Service together on a single host machine using the vCenter Server Simple Install option. See "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.

If you do not enter a license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See the first topic in this multitopic task: "Install vCenter Single Sign On, vCenter Inventory Service, and vCenter Server by Using Simple Install," on page 247.
- See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221
- Install vCenter Single Sign-On and Inventory Service. See "Separately Install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server," on page 251.
- To install the vCenter Server on a drive other than `C:`, verify that there is enough space in the `C:` drive to install the Microsoft Windows Installer `.msi` file.

Procedure

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

2 Select **vCenter Server**™.

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

4 Choose the type of database that you want to use.

- To use the bundled database, click **Install a Microsoft SQL Server 2008 Express instance (for small-scale deployments: up to 5 hosts and 50 virtual machines)**.
- To use an existing database, click **Use an existing supported database** and select your database from the list of available DSNs. Enter the user name and password for the DSN.

  If your database uses Windows NT authentication, the user name and password fields are disabled.

NOTE You might get a warning that the DSN points to an older version of a repository that must be upgraded. If you click **Yes**, the installer upgrades the database schema, making the database irreversibly incompatible with previous VirtualCenter versions. See the *vSphere Upgrade* documentation.

---

5 If the installer prompts you, enter the JDBC URL for your existing vCenter Server database.

The installer should generate and validate the JDBC URL for the vCenter Server database. If the installer fails to connect to the database by using the generated JDBC URL, the installer prompts you to specify the JDBC URL.

6 Set the login information for vCenter Server.

- If you are using a nonbundled database, enter the administrator name and password that you use when you log in to the system on which you are installing vCenter Server.
- If you are using the bundled SQL Server database, select **Use SYSTEM Account**.

You need the user name and password to log in to vCenter Server after you install it.

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

7 Select **Create a standalone VMware vCenter Server instance** or **Join a VMware vCenter Group using Linked Mode to share information**.

Joining a Linked Mode group enables the vSphere Client and vSphere Web Client to view, search, and manage data across multiple vCenter Server systems.

NOTE This option does not appear if you are upgrading the VirtualCenter or vCenter Server database schema. You can join a Linked Mode group after the installation is complete.

8 If you join a group, enter the fully qualified domain name and LDAP port number of any remote vCenter Server system.

9 Enter the port numbers that you want to use or accept the default port numbers.

See "Required Ports for vCenter Server," on page 39.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 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 topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is admin@System-Domain, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 If prompted to install or overwrite a certificate, follow the prompt.

14 Register a vCenter Server administrator with vCenter Single Sign-On, and select the check box if the administrator is a group.

The administrator or group you register here is granted the necessary privileges to administer the vCenter Server instance that you are installing.

15 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

16 Either accept the default destination folder or click **Change** to select another location.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

17 Click **Install**.

Multiple progress bars appear during the installation of the selected components.

18 Click **Finish**.

What to do next

After you install vCenter Server, you can display the vCenter Server welcome page by typing the IP address of the vCenter Server machine or by typing **`localhost`** from a browser installed on the vCenter Server machine. From the welcome page, you can download the vSphere Client. You can also install the vSphere Web Client to access vCenter Server. See "Install or Upgrade the vSphere Web Client," on page 282.

See Chapter 12, "After You Install vCenter Server," on page 279.

vCenter Single Sign-On Installation Fails

In a Windows environment, vCenter Single Sign-On installation might fail for several reasons.

Problem

The vCenter Single Sign-On installation fails in a Windows environment.

Cause

Multiple causes of an installation failure.

Solution

1 Verify that all installation setup prerequisites are met.

   At the time the installation fails, the installer displays a message similar to `####: Installation failed due to....`

2 At a command line, run the following command to gather a vCenter Single Sign-On support bundle.

   `C:\Windows\System32\cscript.exe "`*`SSO Server`*`\scripts\sso-support.wsf" /z`

3 Click **OK**

4 View the logs in *`SSO Server`*`\utils\logs\imsTrace.log, install.log` and `%TEMP%\vminstall.log` for details about the failure and possible solutions.

vCenter Single Sign-On Fails at Start Up or During Initialization

Several problems can cause vCenter Single Sign-On to fail at start up or during initialization.

Problem

vCenter Single Sign-On fails either at start up or during initialization.

Cause

Startup or initialization failures occur in the following situations.

- If your database server is on the same machine as vCenter Single Sign-On, in some cases restarting your machine might cause vCenter Single Sign-On to start before the database server is initialized.
- If you use an external database server, it is possible that the database is not accessible.
- If you use an external database server, the database server login password might have expired or been changed and not updated in vCenter Single Sign-On. Database log-in accounts do not expire using the embedded Microsoft SQL Server Express Database.

Solution

- If vCenter Single Sign-On starts before the database server is initialized, manually restart vCenter Single Sign-On.

- The database server must be accessible using the IP address or FQDN that you used when you installed vCenter Single Sign-On.
  a Find the properties file at *SingleSignOn_Server*\webapps\lookupservice\WEB-INF\classes\config.properties and confirm that the IP address or FQDN is correct.
  b Make any needed changes.
- Verify that the database that vCenter Single Sign-On is configured for use.
  a At a command line, type ***SingleSignOn_server*\utils\ssocli manage-secrets -a listallkeys**
  b When prompted, type the master password.
  c To update the configuration, type **ssocli configure-riat -a configure-db**.

If Autodiscovery Fails During Single Sign-On Installation Manually Add Active Directory Domains

A failure of autodiscovery during vCenter Single Sign-On installation on a machine with a Windows operating system can require you to manually add Active Directory domains.

Problem

vCenter Single Sign-On installation can fail to see Active Domains if autodiscovery fails.

Cause

Autodiscovery failure occurs for several reasons. Some causes are configuration errors with DNS and reverse lookup, trust issues, and certificate problems.

Solution

1 Verify that the network prerequisites are met as described in *vSphere Installation and Setup*.

2 Verify that the DNS configuration is correct.

View the logs at *Single_Sign_On_Server*\utils\logs\discover-is.log and imsTrace.log, or at a command line type ***Single_Sign_On_Server*\utils\ssocli configure-riat -a discover-is** and follow the prompts. If log messages include an error similar to

```
WARNING: Discovered address ‘hostname/ip' does not
map to the same host in reverse lookup.
Host: ‘another_hostname/same ip
```

review the domain controller host DNS configuration and make necessary changes.

3 To expose any connectivity and trust problems, force the server to leave and then rejoin the domain.

4 If your controllers have SSL enabled on LDAP services, verify that the SSL certificate is still valid.

5 If autodiscovery fails, add the Active Directory domain to vCenter Single Sign-On using the vSphere Web Client.

Install vCenter Server in a Virtual Machine

You can install vCenter Server in a Microsoft Windows virtual machine that runs on an ESXi host.

Deploying the vCenter Server system in the virtual machine has the following advantages:

- Rather than dedicating a separate server to the vCenter Server system, you can place it in a virtual machine running on the same host where your other virtual machines run.
- You can provide high availability for the vCenter Server system by using vSphere HA.

- You can migrate the virtual machine containing the vCenter Server system from one host to another, enabling maintenance and other activities.
- You can create snapshots of the vCenter Server virtual machine and use them for backups, archiving, and so on.

Prerequisites

See "Prerequisites for Installing vCenter Single Sign-On, Inventory Service, and vCenter Server," on page 221.

Procedure

1 On any machine that has network access to your ESXi host, install the vSphere Client.

2 Using the vSphere Client, access the ESXi host directly and create the virtual machine for hosting vCenter Server.

3 In the virtual machine, install vCenter Server.

See "Install vCenter Server in a Separate Installation," on page 268.

Download and Deploy the VMware vCenter Server Appliance

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

The vCenter Server Appliance has the default user name **root** and password **vmware**. You can also create a custom password that the vCenter Server Appliance reads on first boot. See "Create a Custom Password on the First Boot for the vCenter Server Appliance," on page 275.

Microsoft SQL Server and IBM DB2 are not supported for the vCenter Server Appliance. The vCenter Server Appliance does not support Linked Mode configuration.Versions 5.0.1 and 5.1 of the vCenter Server Appliance use PostgreSQL for the embedded database instead of IBM DB2, which was used in vCenter Server Appliance 5.0.

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

For information about configuring the vCenter Server Appliance, see the *vCenter Server and Host Management* documentation.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

The ESXi Dump Collector service, the vSphere Syslog service, and vSphere Auto Deploy must use an IPv4 address to communicate with the vCenter Server Appliance.

Prerequisites

- Verify that the host machine meets the hardware requirements for the vCenter Server Appliance listed in "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.
- Verify that the hosts are running ESX version 4.x or ESXi version 4.x or later.
- Synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 232.

- If you plan to configure the vCenter Server Appliance from a configuration file, prepare the file and store it in a location that is accessible from the vCenter Server Appliance host machine. See "Format for the vCenter Server Appliance Configuration File," on page 276.
- See the *vSphere Virtual Machine Administration* documentation for instructions on deploying OVA files and OVF templates.

Procedure

1 From the vSphere 5 download page on the VMware Web site, download the `.OVA` file or the `.OVF` and `VMDK` files for the vCenter Server appliance onto your system.

2 Using the vSphere Client or the vSphere Web Client, deploy the `.OVA` file or the `.OVF` and `VMDK` files as an OVF template.

If you do not want to commit to using the maximum 80GB of disk space at deployment, deploy the vCenter Server Appliance with thin provisioning. In the Disk Format panel of the Deploy OVF template wizard, select **Thin provisioned format**.

3 Power on the vCenter Server Appliance.

4 Open a console view.

5 Follow the instructions on the welcome screen to open a browser window to the URL shown.

6 Log in to the vCenter Server Appliance and accept the license agreement.

When you log in, the vCenter Server Setup wizard starts.

7 Select the configuration option for your installation.

Option	Description
Configure with default settings	Sets up embedded vCenter Server and vCenter Single Sign On databases in the vCenter Server Appliance and configures the databases and Active Directory with default settings.
Upload configuration file	To configure the vCenter Server Appliance from a prepared configuration file.
Set custom configuration	To customize the configuration of the vCenter Server Appliance. The setup wizard displays separate panels for you to connect the appliance to embedded or external vCenter Server and vCenter Single Sign On databases, and to configure custom Active Directory settings.

8 Follow the prompts to complete the wizard.

If you uploaded a configuration file, enter any settings that were not included in the file as you complete the wizard.

NOTE If you set the vCenter Server Apliance to use an external instance of Single Sign On, the external Single Sign On instance must be hosted on another vCenter Server Appliance. It cannot be hosted on a Windows machine.

The vCenter Server Appliance is deployed and set up.

What to do next

See the *vCenter Server and Host Management* documentation for information about using vCenter Server and the vCenter Server Appliance.

Create a Custom Password on the First Boot for the vCenter Server Appliance

The vCenter Server Appliance has the default user name **root** and password **vmware**. You can also create a custom password that the vCenter Server Appliance reads the first time you boot the appliance.

By creating a custom password the first time you start the vCenter Server Appliance, you ensure that the default password cannot be used.

NOTE When you change the root vCenter Server Appliance password using the vCenter Server Appliance Web interface, the GRUB password is changed automatically. However, when you change the vCenter Server Appliance password using the vCenter Server Appliance console, the GRUB password is not changed. You must update the vCenter Server Appliance root password using the Web interface to simultaneously change the GRUB password.

Procedure

1 From a terminal window on your Linux host machine, type the following command to create an MD5 hash of the custom password.

```
grub-md5-crypt
```

2 At the prompt, type the new password and press Enter.

The system returns the MD5 hash of the password.

3 Create a CD directory.

```
mkdir cd
```

4 Add the MD5 hash to the vCenter Server Appliance configuration file.

```
echo 'rootPwdHashMD5=hash_password' > cd/vcva.cfg
```

hash_password is the MD5 hash of the password returned in Step 2. Use single quotes for the echo command, as shown, because the *hash_password* contains $ characters that must be escaped otherwise.

5 Create an ISO file containing the password.

```
mkisofs -R -o rootpass.iso cd
```

6 Attach the CD/DVD drive of the vCenter Server Appliance virtual machine to the `rootpass.iso` file, and make sure that **Connected at power on** is selected.

When you turn on the vCenter Server Appliance, it reads and applies the custom password you created for the root user.

Configure a vCenter Server Appliance to Use the vCenter Single Sign On of a Different vCenter Server Appliance

You can direct one or more vCenter Server Appliances to use the vCenter Single Sign On instance of a single vCenter Server Appliance. This action makes all the vCenter Server instances accessible by the vSphere Web Client of each vCenter Server Appliance.

You can also set a new vCenter Server Appliance to use an external vCenter Single Sign On instance when you run the vCenter Server Setup wizard for a newly deployed vCenter Server Appliance. See "Download and Deploy the VMware vCenter Server Appliance," on page 273.

Prerequisites

- Deploy and configure the vCenter Server Appliance that has the target instance of vCenter Single Sign On. The target instance of Single Sign On must be hosted on another vCenter Server Appliance. It cannot be hosted on a Windows machine.

- Verify that you have the URL of the Lookup Service for the target instance of vCenter Single Sign On.

Procedure

1 Connect to the vCenter Server Appliance from a Web browser.

2 On the **vCenter Server** tab, click **SSO**.

3 Set the **SSO deployment type** to **external**.

4 Under Lookup service location, type the **URL** of the Lookup Service for the target instance of vCenter Single Sign On.

The new vCenter Server Appliance is configured to use the existing vCenter Single Sign On instance, and both vCenter Server instances are accessible by the vSphere Web Client of either vCenter Server Appliance.

What to do next

You can repeat this procedure for multiple vCenter Server Appliances.

Format for the vCenter Server Appliance Configuration File

When you deploy a new vCenter Server Appliance, you can configure the appliance by uploading a configuration file, instead of entering the settings manually in the vCenter Server Setup wizard.

Configuration File Format

Each line of the configuration file supplies the setting for the corresponding entry in the vCenter Center Setup wizard. The values shown here are variables that describe acceptable entries.

NOTE Passwords in the configuration file are stored to disk as plain text. A better practice is to exclude passwords from the configuration file and enter them manually when you complete the vCenter Setup wizard. If you enter passwords in the configuration file, escape any of the following characters by prefixing it with a backslash (\): double quotation mark ("), single quotation mark ('), dollar sign ($), or backslash (\).

```
#vCenter Server Appliance Configuration File v1.0

#Database options
VC_DB_TYPE=embedded or oracle
#Additional database options if VC_DB_TYPE=oracle
VC_DB_SERVER=vCenter Server database server IP address
VC_DB_SERVER_PORT=vCenter Server database server port number
VC_DB_INSTANCE=vCenter Server database server instance name
VC_DB_USER=vCenter Server database user name
VC_DB_PASSWORD=vCenter Server database user's password

#vCenter Single Sign On options
SSO_TYPE=embedded or external
#Additional Single Sign On options if SSO_TYPE=external
SSO_LS_LOCATION=Single Sign On Lookup Service URL
SSO_LS_CERT_THUMBPRINT=Single Sign On Lookup Service certificate thumbprint
SSO_DB_TYPE=embedded or oracle
#Additional Single Sign On options if SSO_DB_TYPE=oracle
SSO_DB_SERVER=Single Sign On database server IP address
SSO_DB_SERVER_PORT=Single Sign On database server port number
SSO_DB_INSTANCE=Single Sign On database instance name
SSO_DB_USER=Single Sign On database user name
SSO_DB_PASSWORD=Single Sign On database user password
SSO_DB_DBA_PASSWORD=Single Sign On database administrator user password
```

```
#Microsoft Active Directory options
VC_AD_STATUS=0 to disable, 1 to enable
#Additional Microsoft Active Directory option if VC_AD_STATUS=1
VC_AD_DOMAIN=Active Directory fully qualified domain name
```

Example: Example Configuration File

This example shows a configuration file for a vCenter Server Appliance that uses an external Oracle vCenter Server database and an external Single Sign On instance.

```
#vCenter Server Appliance Configuration File v1.0

#Database options
VC_DB_TYPE=oracle
VC_DB_SERVER=10.111.11.111
VC_DB_SERVER_PORT=1521
VC_DB_INSTANCE=orcl
VC_DB_USER=VCA-6
VC_DB_PASSWORD=1VCdb_xy!

#vCenter Single Sign On options
SSO_TYPE=external
SSO_LS_LOCATION=https://machinename.corp.com:7444/lookupservice/sdk
SSO_DB_TYPE=oracle
SSO_DB_SERVER=10.222.22.222
SSO_DB_SERVER_PORT=9999
SSO_DB_INSTANCE=ssodb
SSO_DB_USER=sso-d
SSO_DB_PASSWORD=1Db_xy#!
SSO_DB_DBA_PASSWORD=1SSOdba_ab!
SSO_LS_CERT_THUMBPRINT=

#Microsoft Active Directory options
VC_AD_STATUS=0
VC_AD_DOMAIN=
```

12 After You Install vCenter Server

After you install vCenter Server, consider these postinstallation options before adding inventory for the vCenter Server to manage.

General Requirements

- Install the vSphere Client and vSphere Web Client and make sure that you can access the vCenter Server instance.
- When vCenter Server and the database are installed on the same machine, after you reboot the machine, you might need to restart the VMware VirtualCenter Management Webservices service. See "VMware vCenter Management Webservices Service Fails to Start," on page 302.
- Review the subtopics in this section for other postinstallation options.

Oracle Database Requirements

- For the Oracle Instant client, copy ojdbc14.jar to the vCenter Server tomcat directory *vCenter install location*\Infrastructure\tomcat\lib.
- The Oracle 10g client and Oracle 11g client include ojdbc14.jar at: *Install location*\oracle\product\10.2.0*instance_name*\jdbc\lib or *Install location*\app\Administrator\product\11.1.0*instance_name*\sqldeveloper\jdbc\lib. The vCenter Server installer copies the file from the Oracle client installation location to the vCenter Server tomcat directory *vCenter install location*\Infrastructure\tomcat\lib.
- If neither the ojdbc14.jar file nor the ojdbc5.jar file is found in the Oracle 10g or Oracle 11g client location, the vCenter Server installer prompts you to copy the file manually. You can download the file from the Oracle.com Web site.

Security Requirement

For environments that require strong security, VMware recommends that you replace the default certificates on your vCenter Server system with certificates signed by a commercial Certificate Authority (CA). See the information on increasing security for session information in the *vSphere Examples and Scenarios* documentation.

This chapter includes the following topics:

Install vCenter Server Components

You can install vCenter Server components on the same machine that hosts vCenter Server or on remote machines.

Download the vSphere Client

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

Prerequisites

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

The system must have an Internet connection.

Procedure

1 From a Windows machine, open a Web browser.

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

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

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

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

The vSphere Client installer is downloaded to the system.

What to do next

Install the vSphere Client.

Install the vSphere Client

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

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 Run the vSphere Client installer in one of the following ways.

Option	Description
If you are installing from the vCenter Server installer	a In the software installer directory, double-click the `autorun.exe` file. b Select **vSphere™ Client**. c Click **Install**.
If you downloaded the vSphere Client	Double-click the `VMware-viclient-`*`build number`*`.exe` file.

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

You can use the vSphere Client to connect to an ESXi host or to connect to a vCenter Server system.

Start the vSphere Client

After you install the vSphere Client, you can connect to an ESXi host and to a vCenter Server system.

NOTE Do not use the Windows built-in Guest account to start the vSphere Client. By default, the Guest account is disabled. When you use the Guest account to log in to Windows, you cannot access the applications that are already installed on the computer.

Procedure

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

2 In the vSphere Client login window, take one of the following actions.

Option	Description
Log in to an ESXi host.	Log in as root or as a normal user.
Log in to a vCenter Server system as the administrator.	a Type the vCenter Server IP address or host name. b Type your user name and password.

When you connect to the vCenter Server, use 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.

3 Click **Login**.

If you cannot connect to the vCenter Server system, start the VMware VirtualCenter Management Webservices service manually. Select **Settings > Control Panel > Administrative Tools > Services > VMware VirtualCenter Management Webservices** and start the service. The service might require several minutes to start.

4 To ignore the security warnings that appear, click **Ignore**.

Security warning messages appear because the vSphere Client detects certificates signed by the ESXi host or vCenter Server system (default setting).

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage an ESXi host through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client to version 5.1.

NOTE vCenter Server 5.1 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPV4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Client and vSphere Web Client Software Requirements," on page 38.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 232.
- Install vCenter Single Sign On, and install or upgrade Inventory Service and vCenter Server to version 5.1.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.
- If you are upgrading the vSphere Web Client, and you plan to use it with any version 5.0.x vCenter Server instance that was registered to a version 5.0 vSphere Web Client without accepting the SSL thumbprint, see "Version 5.1 vSphere Web Client Fails to Connect to Version 5.0.x vCenter Server," on page 283.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **VMware vSphere® Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Accept or change the default port settings.

5 Enter the information to register the vSphere Web Client with vCenter Single Sign On.

The vCenter Single Sign On administrator user name is admin@System-Domain, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign On. If you entered a different port number when you installed vCenter Single Sign On, use that port number.

NOTE If you installed vCenter Single Sign On in a vCenter Server Appliance, you can enter the Single Sign On Admin user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

6 Click **Install**.

7 Start the vSphere Web Client by doing one of the following actions.

- In a browser, go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- From the Windows Start menu, select **Programs > VMWare > VMware vSphere Web Client > vSphere Web Client**.

What to do next

Install the Client Integration Plug-In in the vSphere Web Client. See "Install the Client Integration Plug-In in the vSphere Web Client," on page 284

If you will use the vSphere Web Client with version 5.0.x vCenter Servers, register those vCenter Servers on the vSphere Web Client Administration Application page in the browser. You do not need to register version 5.1 vCenter Server systems that use the same vCenter Single Sign On server as the vSphere Web Client. The vSphere Web Client can locate such vCenter Server systems by using VMware Lookup Service. For instructions about registering a vCenter Server System with the vSphere Web Client, see the *vCenter Server and Host Management* documentation. If the browser fails to open or to display the Administration Application page correctly, open the application from the Windows **Start** menu: **Programs > VMware > VMware vSphere Web Client > vSphere Administration Application**

Version 5.1 vSphere Web Client Fails to Connect to Version 5.0.x vCenter Server

The version 5.1 vSphere Web Client fails to connect to a version 5.0.x vCenter Server.

Problem

This problem is accompanied by the error message `Failed to verify the SSL certificate for one or more vCenter Server Systems: vCenter_5.0_IP`

Cause

This problem occurs if the version 5.0.x vCenter Server is registered with a version 5.0 vSphere Web Client without accepting the SSL thumbprint, and then the vSphere Web Client is upgraded to version 5.1.

Solution

1 If you have not upgraded the vSphere Web Client to version 5.1, take the following steps.

a Unregister the vCenter Server from the version 5.0 vSphere Web Client.

b Reregister the vCenter Server to the version 5.0 vSphere Web Client and in the Certificate Warning panel, select the check box **Install this certificate and do not display any security warnings for this server** and click **Ignore**.

For instructions about registering and unregistering vCenter Server from a vSphere Web Client, see the *vCenter Server and Host Management* documentation

2 If you have upgraded the vSphere Web Client to version 5.1, take the following steps.

   a Unregister the vCenter Server from the version 5.1 vSphere Web Client.

   b Reregister the vCenter Server to the version 5.1 vSphere Web Client.

   For instructions about registering and unregistering vCenter Server from a vSphere Web Client, see the *vCenter Server and Host Management* documentation

Install the Client Integration Plug-In in the vSphere Web Client

The Client Integration Plug-in provides access to a virtual machine's console in the vSphere Web Client, and provides access to other vSphere infrastructure tasks.

You use the Client Integration Plug-in to deploy OVF or OVA templates and transfer files with the datastore browser. You can also use the Client Integration Plug-in to connect virtual devices that reside on a client computer to a virtual machine.

You install the Client Integration Plug-in only once to connect virtual devices to virtual machines that you access through an instance of the vSphere Web Client. You must restart the browser after you install the plug-in.

If you install the Client Integration Plug-in from an Internet Explorer browser, you must first disable Protected Mode. Internet Explorer identifies the Client Integration Plug-in as being on the Internet instead of on the local intranet. In such cases, the plug-in does not install correctly because Protected Mode is enabled for the Internet.

The Client Integration Plug-in also enables you to log in to the vSphere Web Client using Windows session credentials.

For information about supported browsers and operating systems, see the *vSphere Installation and Setup* documentation.

Procedure

1 Disable Internet Protected Mode for Internet Explorer browsers.

   a Open the browser and select **Tools** > **Internet Options**.

   b Click the **Security** tab and deselect **Enable Protected Mode** for the Internet and Local intranet zones.

2 Click the **Download the client integration plug-in** link.

Option	Description
vSphere Web Client login page	a Open a Web browser and enter the URL for the vSphere Web Client. b At the bottom of the vSphere Web Client login page, click **Download Client Integration Plug-in**.
Guest OS Details panel	a Select a virtual machine in the inventory and click the **Summary** tab. b Click **Download Client Integration Plug-in**.

3 If the browser blocks the installation, either by issuing certificate errors or with pop-up blocking, follow the Help instructions for your browser to resolve the problem.

What to do next

You can open the virtual machine console to configure operating system settings, run applications, monitor performance, and so on.

Install a Local Copy of vSphere Web Client Help

If you do not have internet access from the system you use to access the vSphere Web Client, you can download and deploy a local copy of the online Help.

By default, vSphere Web Client accesses online Help on the Web. This allows the client to access the most up-to-date version of the Help content.

If you download and deploy Help locally, the local copy is not updated when new Help is published to the Web. If you deploy local Help, check the download location periodically for updates.

For instructions for downloading and deploying vSphere Web Client online Help locally, see http://kb.vmware.com/kb/2030344.

Install the Update Manager Server

The Update Manager installation requires a connection with a single vCenter Server instance. You can install Update Manager on the same computer on which vCenter Server is installed or on a different computer.

Prerequisites

See Update Manager installation prerequisites in *Installing and Administering VMware vSphere Update Manager*.

Check the compatibility and interoperability of the vCenter Server server with SRM. You should use caution when connecting the Update Manager server to a vCenter Server instance to which the SRM server is connected. Connecting the Update Manager server to the same vCenter Server instance as SRM might cause problems when you upgrade SRM or vSphere, and when you perform daily operations.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file and select **vSphere Update Manager**.

   If you cannot run `autorun.exe`, browse to the `UpdateManager` folder and run `VMware-UpdateManager.exe`.
2. Select a language for the installer and click **OK**.
3. Review the Welcome page and click **Next**.
4. Read the patent agreement and click **Next**.
5. Accept the terms in the license agreement and click **Next**.
6. Review the support information, select whether to download updates from the default download sources immediately after installation, and click **Next**.

   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 the **Download Now** button on the Download Settings page. You can modify the default download schedule after the installation is complete.

   If you deselect **Download updates from default sources immediately after installation**, the update download task runs after installation, but it does not download any updates.
7. Type the vCenter Server IP address or name, HTTP port, and the administrative account that the Update Manager server will use to connect to the vCenter Server system, and click **Next**.

8 Select the type of database that you want to use.

- If you do not have an existing database, select **Install a Microsoft SQL Server 2008 R2 Express instance (for small scale deployments)** and click **Next**.

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

- If you have a supported database, select **Use an existing supported database** and select a DSN from the drop-down menu. If the DSN does not use Windows NT authentication, type the user name and password for the DSN and click **Next**.

  IMPORTANT The DSN must be a 32-bit DSN.

9 (Optional) Select the database options.

- If the system DSN you specify points to an existing Update Manager database with the current schema, you can either retain your existing database or replace it with an empty one.
- If the system DSN you specify points to an existing Update Manager database with different schema, 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**.

10 From the drop-down menu, select the IP address or the host name of your Update Manager instance.

If the computer on which you install Update Manager has one NIC, the Update Manager installer automatically detects the IP address. If the computer has multiple NICs, you must select the correct IP address or use a DNS name. The DNS name must be resolved from all hosts that this Update Manager instance will manage.

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

NOTE Use caution when you specify the Update Manager port settings, as you cannot modify them after installation.

For the SOAP port, you have no limitations to the range of ports used, as long as there are no conflicts.

For the Server port, you can use the following range: 80, 9000-9100. Update Manager automatically opens SX/ESXi firewall ports in this range to allow outbound HTTP traffic to the patch store.

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

13 Select the Update Manager installation and patch download directories, and click **Next**.

If you do not want to use the default locations, you can click **Change** to browse to a different directory.

14 (Optional) In the warning message about the disk free space, click **OK**.

This message appears when you try to install Update Manager on a computer that has less than 120GB free space.

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

16 Click **Finish**.

The Update Manager server component is installed, and the client component appears as an available plug-in in the Plug-in Manager of the vSphere Client.

What to do next

In the vSphere Client, select **Plug-ins > Manage Plug-ins** to install and enable the Update Manager Client plug-in.

Install or Upgrade vSphere ESXi Dump Collector

You can configure ESXi to dump the vmkernel memory to a network server, rather than to a disk, when the system has encountered a critical failure. Install vSphere ESXi Dump Collector to collect such memory dumps over the network.

If an earlier version of the Dump Collector is installed on your system, this procedure upgrades the Dump Collector to version 5.1.

NOTE In the vCenter Server Appliance, the ESXi Dump Collector is installed and enabled by default. These instructions apply to Windows-based deployments.

For instructions on configuring ESXi to dump kernel memory to the network server, see "Configure ESXi Dump Collector with ESXCLI," on page 99.

The Dump Collector is most useful for datacenters where ESXi hosts are configured using the Auto Deploy process, so it might not have local storage. You can also install the Dump Collector for ESXi hosts that do have local storage, as an additional location where vmkernel memory dumps can be redirected when critical failures occur.

You can install the Dump Collector on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. ESXi Dump Collector does not support vSphere distributed switches in ESXi 5.x.

The Dump Collector service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Client must have an IPv4 address for the Dump Collector service to work.

Prerequisites

- Verify that you have administrator privileges
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. The Dump Collector supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 37 and "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.
- Verify that the host machine has a valid IPv4 address. You can install the Dump Collector on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install the Dump Collector on a machine in an IPv6-only environment.
- If you are using a network location for the Dump Collector repository, make sure the network location is mounted.

Gather the following information to complete the installation or upgrade:

- The location to install the Dump Collector to, if you are not using the default location.
- The location for the Dump Collector repository where the dump files will be stored.
- (Optional) The maximum size for the Dump Collector repository. The specified network location must have at least that much free space.
- Whether to install the Dump Collector as a standalone instance or to integrate the Dump Collector with a vCenter Server. The Dump Collector is not supported for integration with vCenter Server versions earlier than version 5.0.
- If the Dump Collector is integrated with a vCenter Server, the address and credentials for the vCenter Server: IP address or name, HTTP port, user name, and password.

- The Dump Collector server port, if you are not using the default setting.
- The host name or IP address to identify the Dump Collector on the network.

Procedure

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

2 Select **VMware vSphere®ESXi™Dump Collector** and click **Install**.

3 Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade vSphere Syslog Collector

Install the vSphere Syslog Collector to enable ESXi system logs to be directed to a server on the network, rather than to a local disk.

If an earlier version of the Syslog Collector is installed on your system, this procedure upgrades the Syslog Collector to version 5.1.

You can install the Syslog Collector on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. The Syslog Collector service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Client must have an IPv4 address for the Syslog Collector service to work.

Prerequisites

- Verify that you have administrator privileges.
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. The Syslog Collector supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 37 and "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.
- Determine whether to install the Syslog Collector as a standalone instance or to integrate the Syslog Collector with a vCenter Server. The Syslog Collector is not supported for integration with vCenter Server versions earlier than version 5.0.
- Verify that the host machine has a valid IPv4 address. You can install the Syslog Collector on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install the Syslog Collector on a machine in an IPv6-only environment.

Gather the following information to complete the installation or upgrade:

- The location to install the Syslog Collector to, if you are not using the default location.
- The location for the Syslog Collector repository where the syslog files will be stored.
- (Optional) The maximum size for the Syslog Collector repository. The specified network location must have at least that much free space.
- (Optional) The maximum number of Syslog Collector log rotations to keep.
- If the Syslog Collector is integrated with a vCenter Server, the address and credentials for the vCenter Server: IP address or name, HTTP port, user name, and password.
- The Syslog Collector server port, if you are not using the default setting, and whether to use TCP and UDP protocols for this port.
- The Syslog Collector server SSL port, if you are not using the default setting, and whether to use secure connection (SSL) for this port.

- The host name or IP address to identify the Syslog Collector on the network.

Procedure

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

2 Select **VMware vSphere® Syslog Collector** and click **Install**.

3 Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade vSphere Auto Deploy

Install vSphere Auto Deploy to provision and customize physical hosts by loading the ESXi image directly into memory. You can provision and reprovision hundreds of ESXi hosts efficiently with vCenter Server.

If an earlier version of Auto Deploy is installed on your system, this procedure upgrades Auto Deploy to version 5.1.

You must install the Auto Deploy server separately for each instance of vCenter Server that you plan to use the Auto Deploy with. Auto Deploy is not supported with vCenter Server versions earlier than version 5.0. Using vCenter Server 5.1 with Auto Deploy 5.0 is not supported. You must upgrade Auto Deploy to version 5.1 for use with vCenter Server 5.1. Auto Deploy supports both IPv4 and IPv6. However, Auto Deploy uses a PXE boot infrastructure that supports only IPv4. You can use Auto Deploy in a mixed IPv4-IPv6 environment or an IPv4-only environment, but not in an IPv6-only environment.

Prerequisites

- Verify that you have administrator privileges
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. Auto Deploy supports the same processors and operating systems as vCenter Server.

  See "vCenter Server Software Requirements," on page 37 and "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.

Gather the following information to complete the installation or upgrade:

- The location to install Auto Deploy in, if you are not using the default location.
- The location for the Auto Deploy repository. Do not use a network share for the repository.
- (Optional) The maximum size for the Auto Deploy repository. Best practice is to allocate 2GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350MB. Determine how much space to reserve for the Auto Deploy repository by considering how many image profiles you expect to use. The specified disk must have at least that much free space.
- The address and credentials of the vCenter Server that you are installing the Auto Deploy feature for: IP address or name, HTTP port, user name, and password.
- The Auto Deploy server port, if you are not using the default setting.
- The host name or IP address to identify Auto Deploy on the network.

Procedure

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

2 Select **VMware vSphere® Auto Deploy** and click **Install**.

3 Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade VMware vSphere Authentication Proxy

Install vSphere Authentication Proxy to enable ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy, by removing the need to store Active Directory credentials in the host configuration.

If an earlier version of the vSphere Authentication Proxy is installed on your system, this procedure upgrades the vSphere Authentication Proxy to version 5.1.

You can install vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. The vSphere Authentication Proxy is not supported with vCenter Server versions earlier than version 5.0.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Install vSphere Auto Deploy. See "Install or Upgrade vSphere Auto Deploy," on page 289.
- Verify that you have administrator privileges.
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. vSphere Authentication Proxy supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 37 and "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.
- Verify that the host machine has a valid IPv4 address. You can install vSphere Authentication Proxy on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install vSphere Authentication Proxy on a machine in an IPv6-only environment.
- If you are installing vSphere Authentication Proxy on a Windows Server 2008 R2 host machine, download and install the Windows hotfix described in Windows KB Article 981506 on the support.microsoft.com Web site. If this hotfix is not installed, the Authentication Proxy Adapter fails to initialize. This problem is accompanied by error messages in `camadapter.log` similar to `Failed to bind CAM website with CTL` and `Failed to initialize CAMAdapter.`

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Authentication Proxy, if you are not using the default location.
- The address and credentials for the vCenter Server that vSphere Authentication Proxy will connect to: IP address or name, HTTP port, user name, and password.
- The host name or IP address to identify vSphere Authentication Proxy on the network.

Procedure

1. On the host machine where you will install the vSphere Authentication Proxy service, install the .NET Framework 3.5.
2. Install vSphere Auto Deploy.

   You do not have to install Auto Deploy on the same host machine as the vSphere Authentication Proxy service.
3. Add the host machine where you will install the authentication proxy service to the domain.
4. Use the Domain Administrator account to log in to the host machine.

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

6 Select **VMware vSphere® Authentication Proxy** and click **Install**.

7 Follow the wizard prompts to complete the installation or upgrade.

During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

When you install the vSphere Authentication Proxy service, the installer creates a domain account with appropriate privileges to run the authentication proxy service. The account name begins with the prefix `CAM–` and has a 32-character, randomly generated password associated with it. The password is set to never expire. Do not change the account settings.

What to do next

Configure ESXi to use vSphere Authentication Proxy to join a domain. See the *vSphere Security* documentation.

Uninstall VMware vSphere Components

The VMware vSphere components and Support Tools are uninstalled separately, even if they are on the same machine. You must have administrator privileges to uninstall VMware vCenter Server

Caution Uninstalling a vCenter Server system while it is running disrupts the vSphere Client connections, which can cause data loss.

Uninstalling the vCenter Server system or the vSphere Client does not uninstall any of the other components, such as the bundled database or Microsoft .NET Framework. Do not uninstall the other components if other applications on your system depend on them.

Procedure

1 If you are uninstalling the vCenter Server system, remove the hosts from the Hosts and Clusters inventory.

2 As Administrator on the Microsoft Windows system, select **Start > Settings > Control Panel > Add/Remove Programs**.

3 Select the component to remove from the list and click **Remove**.

4 Click **Yes** to confirm that you want to remove the program.

5 Click **Finish.**

Back Up the vCenter Single Sign On Configuration

Maintain a current backup of the Single Sign On configuration. If your Single Sign On instance is corrupted, you can restore the backup to ensure continued vSphere access for vCenter Server and vCenter Server components.

Back up the Single Sign On configuration in the following circumstances.

- After you install, update, or change the location of a vCenter Single Sign On instance.
- When the `node.pkg` file is modified. The `node.pkg` file is modified when you take either of the following actions.
  - Change Single Sign On database information, such as the database host name or port.
  - Change the Single Sign On password that was created for the administrator user admin@System-Domain when Single Sign On was originally installed. This original password is required when you restore a Single Sign On backup.

For a complete backup, you must also back up your Single Sign On database. See the documentation for your database type.

Procedure

- On the vCenter Single Sign On host machine, take one of the following actions.

Option	Description
From the Windows user interface	a Go to **Programs > VMware**. b Right-click **Generate vCenter Single Sign On backup bundle** and select **Run as administrator**.
From a command prompt	a Right-click the **Command Prompt** icon or menu item, and select **Run as administrator**. b Change directory to `C:\Program Files\VMware\Infrastructure\SSOServer\scripts`. If you installed Single Sign On in a location other than the default `C:\Program Files`, adjust the path. c Type `cscript sso-backup.wsf /z` and press Enter.

The vCenter Single Sign On configuration is backed up as `Single Sign On.zip` on the Desktop of the host machine. To restore a vCenter Single Sign On backup, see "Restore a vCenter Single Sign On Single or Primary Node Instance to a New Host Machine," on page 292.

Restore a vCenter Single Sign On Single or Primary Node Instance to a New Host Machine

If your vCenter Single Sign On single node or primary node instance is corrupted, you can restore a backup to ensure continued vSphere access for vCenter Server and vCenter Server components.

Prerequisites

- Verify that you have a current backup of your vCenter Single Sign On configuration. See "Back Up the vCenter Single Sign On Configuration," on page 291.
- Prepare a host machine for the restored Single Sign On instance. The host machine can be a physical machine or a virtual machine. It must satisfy the hardware requirements for Single Sign On. See "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.
- Verify that the vCenter Single Sign On database is accessible from the host machine.
- Verify that you have the original administrator password for the vCenter Single Sign On instance that you are restoring.
- Verify that you have the account name and password for the RSA SSPI service and vCenter Single Sign On service of the vCenter Single Sign On instance that you are restoring.
- Download the vCenter Server installer from the VMware downloads page at http://www.vmware.com/support/ to the new host machine.

Procedure

1. Copy the backup file `Single Sign On.zip` to the new host machine in the directory `C:\Temp\SSO Recovery`.
2. Rename the new host with the same Fully Qualified Domain Name (FQDN) as the Single Sign On server that you created the backup from.
3. If the Single Sign On instance that you created the backup from was in a workgroup, and was installed using its IPv4 address, make sure that the new host machine has the same static IP address.

   DHCP is not supported.

4 Verify that the DNS of the new host is forward and reverse resolvable.

5 On the vCenter Single Sign On host machine, in the VMware vCenter Server installation directory, double-click the `autorun.exe` file to start the installer.

6 Select **vCenter™Single Sign On** and click **Install**.

7 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

8 Select **Recover installed instance of vCenter Single Sign On from a backup**.

9 Browse to and select the `Single Sign On.zip` file.

10 Enter the original administrator password for the old Single Sign On instance.

   You must use the password that was created for the admin@System-Domain user when Single Sign On was originally installed, even if you have changed that password.

11 Make sure that the RSA SSPI service is logged on to the same account as in the Single Sign On instance that you created the backup from.

12 Follow the wizard prompts to complete the Single Sign On restoration.

The vCenter Single Sign On single or primary node instance is restored.

What to do next

If there are any Single Sign On high availability backup nodes associated with the primary node that you restored, make sure that the RSA SSPI service logs on to the same account in the primary node and all high availability backup nodes.

From the vSphere Web Client, log in to the vCenter Server instances that are registered to the Single Sign On instance to verify that you have working access to them.

Creating vCenter Server Linked Mode Groups

A Linked Mode group allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group.

You can join multiple vCenter Server systems to form a Linked Mode group. You can configure a Linked Mode group during vCenter Server installation or after vCenter Server is installed.

To join a vCenter Server group, you enter the fully qualified domain name (or IP address) of a remote machine on which vCenter Server is running. The remote machine can be any vCenter Server instance that is, or will become, a member of the Linked Mode group.

You must also provide the LDAP port number of the remote vCenter Server instance.

vCenter Server instances in a group replicate shared global data to the LDAP directory. The global data includes the following information for each vCenter Server instance:

- Connection information (IP and ports)
- Certificates
- Licensing information
- User roles

The vSphere Web Client can connect to a Linked Mode vCenter Server environment only if the vSphere Web Client is logged in to vCenter Server as a domain user. For example, if the Linked Mode vCenter Servers are installed with user "abc" added to domain "xyz," the vSphere Web Client user should log in using **xyz\abc**.

NOTE vCenter Server 5.1 can be joined in a Linked Mode group only with other instances of vCenter Server 5.1. Do not join a version 5.1 vCenter Server instance to a version 5.0 or earlier vCenter Server instance.

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 are upgrading a version 5.0.x 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.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain both version 5.1.x and 5.0.x versions of vCenter Server. vCenter Server 5.0.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.0.x. vCenter Server 5.1.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.1.x. After all vCenter Servers in the group are upgraded to version 5.0.x or all vCenter Servers in the group are upgraded to version 5.1.x, 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.

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 294.

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:

- vCenter Server does not support Linked Mode groups that contain both version 5.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain both version 5.1.x and 5.0.x versions of vCenter Server. vCenter Server 5.0.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.0.x. vCenter Server 5.1.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.1.x. After all vCenter Servers in the group are upgraded to version 5.0.x or all vCenter Servers in the group are upgraded to version 5.1.x, you can rejoin them.
- Make sure that all vCenter Servers in a Linked Mode group are registered to the same vCenter Single Sign On 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. See "Synchronizing Clocks on the vSphere Network," on page 232.

Joining a Linked Mode Group During and After Installation

You can join a system to a Linked Mode group during the vCenter Server installation or after you install vCenter Server.

For example, suppose you have three machines on which you want to install vCenter Server. You want the three instances to be members of a Linked Mode group.

1. On Machine 1, you install vCenter Server as a standalone instance because you do not have a remote vCenter Server machine to join.
2. On Machine 2, you install vCenter Server, choose to join a Linked Mode group, and provide the fully qualified domain name of Machine 1.
3. On Machine 3, you upgrade to vCenter Server 5.x. After the upgrade, you configure Machine 3 to join either Machine 1 or Machine 2. Machine 1, Machine 2, and Machine 3 are now members of a Linked Mode group.

Join a Linked Mode Group After Installation

After installing vCenter Server, you can join a vCenter Server to a Linked Mode group.

Prerequisites

See "Linked Mode Prerequisites for vCenter Server," on page 294 .

NOTE vCenter Server does not support Linked Mode groups that contain both version 5.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain both version 5.1.x and 5.0.x versions of vCenter Server. vCenter Server 5.0.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.0.x. vCenter Server 5.1.x can be joined in a Linked Mode group only with other instances of vCenter Server 5.1.x. After all vCenter Servers in the group are upgraded to version 5.0.x or all vCenter Servers in the group are upgraded to version 5.1.x, you can rejoin them.

Procedure

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

2 Click **Next**.

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

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

5 Enter the server name and LDAP port number of a remote vCenter Server instance that is a member of the group and click **Next**.

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

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

Option	Action
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 one of the vCenter Server systems using an account with **Administrator** privileges. b Rename the conflicting role. c Close the vSphere Client session and return to the vCenter Server installer. d Click **Back** and click **Next**. The installation continues without conflicts.

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

7 Click **Finish**.

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

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

For information about configuring and using your Linked Mode group, see the *vCenter Server and Host Management* documentation.

Isolate a vCenter Server Instance from a Linked Mode Group

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

Procedure

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

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

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

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

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

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

Configure the URLs on a Linked Mode vCenter Server System

If you connect a vCenter Server system to a Linked Mode group and the vCenter Server system has a machine name that does not match the domain name, several connectivity problems arise. Correct this situation by changing the URLs.

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

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

Procedure

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

See "Isolate a vCenter Server Instance from a Linked Mode Group," on page 297

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

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

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

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

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

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

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

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

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

See "Join a Linked Mode Group After Installation," on page 296.

The URLs are now correctly configured.

Set the IP Address for a Linked Mode vCenter Server with Multiple Network Interfaces

If a vCenter Server in a Linked Mode group has multiple network interfaces, you must set the IP address that the vCenter Server advertises to the other vCenter Servers in the Linked Mode group.

Unless you set the IP address, vSphere Client searches, lists, and sorting will not work properly. Also, the vSphere Web Client will not work properly with the vCenter Server.

Procedure

1 On the vCenter Server host machine, using a text editor, open the file *Inventory_Service_installation_directory*`/lib/server/config/query-server-config.xml`.

2 Find the following line.

```
!-- <property name="externalAddress" value="192.168.0.1" /> /--
```

3 Change the line as follows.

```
<property name="externalAddress" value="IP_address" />
```

IP_address is the IP address of this machine on a subnet that will be used to communicate with other vCenter Server instances in the Linked Mode group.

4 Restart the vCenter Inventory Service.

a In the **Administrative Tools** control panel, select **Services**.

b Right-click vCenter Inventory Service and select **Start**.

The status changes to Started.

The IP address is configured.

Linked Mode Troubleshooting

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

When you have multiple vCenter Server instances, each instance must have a working relationship with the domain controller and not conflict with another machine that is in the domain. Conflicts can occur, for example, when you clone a vCenter Server instance that is running in a virtual machine and you do not use sysprep or a similar utility to ensure that the cloned vCenter Server instance has a globally unique identifier (GUID).

If the domain controller is unreachable, vCenter Server might be unable to start. You might be unable to change the Linked Mode configuration of the affected vCenter Server system. If this occurs, resolve the problem with the domain controller and restart vCenter Server. If resolving the problem with the domain controller is impossible, you can restart vCenter Server by removing the vCenter Server system from the domain and isolating the system from its current Linked Mode group.

The DNS name of the machine must match with the actual machine name. Symptoms of machine names not matching the DNS name are data replication problems, ticket errors when trying to search, and missing search results from remote instances.

NOTE Make sure your Windows and network-based firewalls are configured to allow Linked Mode.

Configure a Windows Firewall to Allow a Specified Program Access

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

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

Prerequisites

- The Windows version must be earlier than Windows Server 2008. For Windows Server 2008, Windows automatically configures the firewall to permit access.
- No network-based firewalls can exist between vCenter Server Linked Mode instances. For environments with network-based firewalls, see "Configure Firewall Access by Opening Selected Ports," on page 299.

Procedure

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

Configure Firewall Access by Opening Selected Ports

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

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

Procedure

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

  Choose one of the following methods.

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

Configuring VMware Tomcat Server Settings in vCenter Server 5.1

Starting with vCenter Server 5.1, VMware Tomcat Server settings can no longer be configured through the Windows user interface. vCenter Server 5.1 uses VMware vFabric tc Server, an enterprise version of Apache Tomcat 7. Tomcat version 7 does not provide a control panel in the Windows user interface. Instead, you configure Tomcat by editing configuration files manually.

You can adjust the JVM maximum heap size for vCenter Server, vCenter Single Sign On, vCenter Inventory Service, and Profile-Driven Storage Service. For JVM heap size recommendations, see "Hardware Requirements for vCenter Server, vCenter Single Sign On, vSphere Client, and vSphere Web Client," on page 33.

Settings for Java options are stored in the following files.

- vCenter Server. *installation_directory*\VMware\Infrastructure\tomcat\conf\wrapper.conf
- vCenter Single Sign On. *installation_directory*\VMware\Infrastructure\SSOServer\conf\wrapper.conf
- vCenter Inventory Service. *installation_directory*\VMware\Infrastructure\Inventory Service\conf\wrapper.conf
- Profile-Driven Storage Service. *installation_directory*\VMware\Infrastructure\Profile-Driven Storage\conf\wrapper.conf

Table 12-1. vCenter Server and vCenter Single Sign On Java Maximum JVM Heap Size Setting in the `wrapper.conf` Files

Java Option	Setting and Default Value
-Xmx*size* The maximum JVM heap size, in megabytes. This setting controls the maximum size of the Java heap. Tuning this parameter can reduce the overhead of garbage collection, improving server response time and throughput. For some applications, the default setting for this option is too low, resulting in a high number of minor garbage collections.	`wrapper.java.additional.9="-Xmx1024M"`

Table 12-2. Inventory Service and Profile-Driven Storage Service Java Maximum JVM Heap Size Setting in the `wrapper.conf` Files

Java Option	Setting and Default Value
maxmemory*size* The maximum JVM heap size, in megabytes. This setting controls the maximum size of the Java heap. Tuning this parameter can reduce the overhead of garbage collection, improving server response time and throughput. For some applications, the default setting for this option is too low, resulting in a high number of minor garbage collections.	Inventory Service: `wrapper.java.maxmemory=2048` Profile-Driven Storage Service: `wrapper.java.maxmemory=1024`

vCenter Server and Single Sign On security and port settings are stored in the following files.

- vCenter Server. *installation_directory*\VMware\Infrastructure\tomcat\conf\server.xml and *installation_directory*\VMware\Infrastructure\tomcat\conf\catalina.properties
- vCenter Single Sign On. *installation_directory*\VMware\Infrastructure\SSOServer\conf\server.xml and *installation_directory*\VMware\Infrastructure\SSOServer\conf\catalina.properties

Table 12-3. vCenter Server Port and Security Settings in the `server.xml` and `catalina.properties` Files

vCenter Server Port or Security Setting	Setting and Default Value
Base shutdown port	base.shutdown.port=8003
Base JMX port. The listener implemented by the com.springsource.tcserver.serviceability.rmi.JmxSocketListener class is specific to tc Server. This listener enables JMX management of tc Server, and is the JMX configuration that the AMS management console uses to manage tc Server instances. The port attribute specifies the port of the JMX server that management products, such as AMS, connect to. The variable *${jmx.port}* is set to 6969 in the default `catalina.properties` file. The bind attribute specifies the host of the JMX server. By default, this attribute is set to the localhost (127.0.0.1). The default -1 setting disables the port.	base.jmx.port=-1
Web services HTTPS	bio-vmssl.http.port=8080
Web services HTTPS	bio-vmssl.https.port=8443
SSL certificate	bio-vmssl.keyFile.name=C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.pfx
SSL certificate password	bio-vmssl.SSL.password=testpassword
AJP port	bio-vmssl.ajp.port=8009

Table 12-4. vCenter Single Sign On Port and Security Settings in the `server.xml` and `catalina.properties` Files

vCenter Single Sign On Port or Security Setting	Setting and Default Value
Base shutdown port	base.shutdown.port=7005
Base JMX port. The listener implemented by the com.springsource.tcserver.serviceability.rmi.JmxSocketListener class is specific to tc Server. This listener enables JMX management of tc Server, and is the JMX configuration that the AMS management console uses to manage tc Server instances. The port attribute specifies the port of the JMX server that management products, such as AMS, connect to. The variable *${jmx.port}* is set to 6969 in the default `catalina.properties` file. The bind attribute specifies the host of the JMX server. By default, this attribute is set to the localhost (127.0.0.1). The default -1 setting disables the port.	base.jmx.port=-1
HTTP port	ajp-vm.http.port=7080
HTTPS port	ajp-vm.https.port=7444
AJP port	ajp-vm.ajp.port=7009

See *Getting Started with vFabric tc Server* and *vFabric tc Server Administration* at https://www.vmware.com/support/pubs/vfabric-tcserver.html.

You can manage the Windows services for vCenter Server and vCenter Single Sign On from the Administrative Tools control panel, under Services. The Windows service for vCenter Server is listed as VMware VirtualCenter Management Webservices.

VMware vCenter Management Webservices Service Fails to Start

When you reboot the vCenter Server machine after installing vCenter Server, the VMware VirtualCenter Management Webservices service does not start.

Problem

The VMware VirtualCenter Management Webservices service does not start automatically.

Cause

This problem can occur when vCenter Server and the database are installed on the same machine.

Solution

- Start the service manually.

  Select **Settings > Control Panel > Administrative Tools > Services > VMware VirtualCenter Management Webservices** and start the service. The machine might require several minutes to start the service.

Back Up the Inventory Service Database on Windows

You should back up the Inventory Service database as part of your regular vCenter Server database administration.

To move the Inventory Service database to a different host machine, back up the database on the source machine and restore the database on the destination machine. Your vCenter Server database administration should also include regular backups of your vCenter Server database. See the vendor documentation for your vCenter server database type.

Prerequisites

- Consult your database administrator about backing up and restoring databases.
- Verify that you have system administrator privileges to perform backup or restore operations.

Procedure

1. On the source machine, stop the Inventory Service.
   a. From the Windows Administrative Tools control panel, select **Services**.
   b. Right-click **VMware vCenter Inventory Service** and select **Stop**.

      The Status changes from Started to blank.
2. On the source machine, open the command prompt in the vCenter Server and change the directory to *vCenter_Server_installation_directory*\Infrastructure\Inventory Service\scripts.
3. Run the following command at the prompt to back up the Inventory Service database.

   ```
   backup.bat –file backup_file_name
   ```

   When the backup operation finishes, the message `Backup completed successfully` appears.

Restore an Inventory Service Database Backup on Windows

You can restore a backup of your Inventory Service database for disaster recovery, after a vCenter Server upgrade, or to move the database to a new machine.

The machine that you back up the database from is the source machine. The machine that you restore the database to is the destination machine.

Prerequisites

- Consult your database administrator about backing up and restoring databases.
- Verify that you have system administrator privileges to perform backup or restore operations.

Procedure

1 On the destination machine, stop the Inventory Service.

   a From the Windows Administrative Tools control panel, select **Services**.

   b Right-click **VMware vCenter Inventory Service** and select **Stop**.

   The Status changes from Started to blank.

2 On the destination machine, open the command prompt in the vCenter Server and change the directory to `vCenter Server install location\Infrastructure\Inventory Service\scripts`.

3 Run the following command at the command prompt to restore the Inventory Service database.

   `restore –backup` *`backup_file_name`*

   When the restore operation finishes, the message `The Restore completed successfully message` appears.

Back Up the Inventory Service Database on Linux

You should back up the Inventory Service database as part of your regular vCenter Server database administration.

To move the Inventory Service database to a different host machine, back up the database on the source machine and restore the database on the destination machine.

Prerequisites

- Consult your database administrator about backing up and restoring databases.
- Verify that you have system administrator privileges to perform backup or restore operations.

Procedure

1 On the source machine, open a console and run the `service vmware-inventory service stop` command to stop the Inventory Service before you restore the Inventory Service database.

2 On the source machine, open a command prompt in the vCenter Server and change the directory to `/usr/lib/vmware-vpx/inventoryservice/scripts/`.

3 Run the following command to back up the Inventory Service database.

   `./backup.sh –file` *`backup_file_name`*

   When the backup operation finishes, the message `Backup completed successfully` appears.

What to do next

See "Restore an Inventory Service Database Backup on Linux," on page 303.

Restore an Inventory Service Database Backup on Linux

You can restore a backup of your Inventory Service database for disaster recovery, after a vCenter Server upgrade, or to move the database to a new machine.

The machine that you back up the database from is the source machine. The machine that you restore the database to is the destination machine.

Prerequisites

- Consult your database administrator about backing up and restoring databases.
- Verify that you have system administrator privileges to perform backup or restore operations.

Procedure

1 On the destination machine, open a console and run the `service vmware-inventory service stop` command to stop the Inventory Service before you restore the Inventory Service database.

2 On the destination machine, open a command prompt in the vCenter Server and change the directory to `/usr/lib/vmware-vpx/inventoryservice/scripts/`.

3 Run the following command at the prompt to restore the Inventory Service database.

```
./restore.sh -backup backup_file_name
```

When the restore operation finishes, the message `The Restore completed successfully message` appears at the command prompt.

Reset the vCenter Inventory Service Database

If the vCenter Inventory Service Database is corrupted or otherwise inoperable, you can reset it. You should also reset the vCenter Inventory Service Database if you reset the vCenter Server database.

Caution Resetting the vCenter Inventory Service Database can cause data loss. Perform this procedure only with VMware Technical Support.

Procedure

1 Stop the vCenter Inventory Service.

   a From the Windows Administrative Tools control panel, select **Services**.

   b Right-click **VMware vCenter Inventory Service** and select **Stop**.

2 Open a command prompt.

3 Delete the entire contents of the `C:\Program Files\VMware\Infrastructure\Inventory_Service\data` directory.

   If you installed vCenter Server in a different location from the default `C:\Program Files\`, adjust the path accordingly.

4 Change directory to `C:\Program Files\VMware\Infrastructure\Inventory_Service\scripts`

   If you installed vCenter Server in a different location from the default `C:\Program Files\`, adjust the path accordingly.

5 Run the `createDB.bat` command, with no arguments, to reset the vCenter Inventory Service database.

6 Start the vCenter Inventory Service.

   a From the Windows Administrative Tools control panel, select **Services**.

   b Right-click **VMware vCenter Inventory Service** and select **Start**.

7 Change directory to `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\isregtool`.

   If you installed vCenter Server in a different location from the default `C:\Program Files\`, adjust the path accordingly.

8 Run the `register-is.bat` command to update the stored configuration information of the Inventory Service.

`register-is.bat` *`vCenter_Server_URL Inventory_Service_URL Lookup_Service_URL`*

Use the following example as a model.

```
register-is.bat https://machinename.corp.com:443/sdk https://machinename.corp.com:10443
https://machinename.corp.com:7444/lookupservice/sdk
```

In this example, 443, 10443, and 7444 are the default HTTPS port numbers for vCenter Server, Inventory Service, and vCenter Single Sign On respectively. If you use custom ports, replace the port numbers in the example with the port numbers you use.

9 Restart vCenter Server.

The vCenter Inventory Service database is reset.

Enable IPv6 Support for vCenter Inventory Service

vCenter Inventory Service does not support binding on IPv6 interfaces by default. When you install vCenter Server, vCenter Inventory Service supports only IPv4 by default. You can enable IPv6 support for vCenter Inventory Service by modifying the Inventory Service `dataservice.properties` file.

Procedure

1 Stop the vCenter Inventory Service.

a From the Administrative Tools control panel, select **Services**.

b Right-click **vCenter Inventory Service** and select **Stop**.

2 In a text editor, open the file:*`Inventory_Service_installation_directory`*`/lib/server/config/dataservice.properties`.

3 Change the line `dataservice.nio.enabled = true` to `dataservice.nio.enabled = false`

4 Restart the vCenter Inventory Service.

IPv6 support for vCenter Inventory Service is enabled.

Index

B

C

D

E

F

G

H

L

M

N

O

P

R

S

T

U

V

W