

# vSphere Installation and Setup

vSphere 5.0 Update 1

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

EN-000783-01

**vmware**<sup>®</sup>

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](mailto:docfeedback@vmware.com)

Copyright © 2009–2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

About vSphere Installation and Setup	7
Updated Information	9
<b>1 Introduction to vSphere Installation and Setup</b>	<b>11</b>
How vSphere 5.0 Differs from vSphere 4.x	11
Overview of the vSphere Installation and Setup Process	13
Options for Installing ESXi	14
Media Options for Booting the ESXi Installer	15
Using Remote Management Applications	26
Required Information for ESXi Installation	26
<b>2 System Requirements</b>	<b>29</b>
ESXi Hardware Requirements	29
ESXi Support for 64-Bit Guest Operating Systems	32
vCenter Server and vSphere Client Hardware Requirements	33
vCenter Server Software Requirements	36
vSphere Client and vSphere Web Client Software Requirements	37
Providing Sufficient Space for System Logging	37
Required Ports for vCenter Server	38
Required Ports for the vCenter Server Appliance	39
Conflict Between vCenter Server and IIS for Port 80	40
DNS Requirements for vSphere	40
Supported Remote Management Server Models and Minimum Firmware Versions	41
<b>3 Installing ESXi Interactively</b>	<b>43</b>
Install ESXi Interactively	43
Install ESXi on a Software iSCSI Disk	45
<b>4 Installing, Upgrading, or Migrating Hosts Using a Script</b>	<b>47</b>
Approaches for Scripted Installation	47
Enter Boot Options to Start an Installation or Upgrade Script	48
About Installation and Upgrade Scripts	50
Install, Upgrade, or Migrate ESXi from a CD or DVD Using a Script	59
Install, Upgrade, or Migrate ESXi from a USB Flash Drive Using a Script	60
Performing a Scripted Installation or Upgrade of ESXi by PXE Booting the Installer	61
<b>5 Installing ESXi Using vSphere Auto Deploy</b>	<b>63</b>
Understanding vSphere Auto Deploy	63
Auto Deploy Roadmap and Cmdlet Overview	70
Preparing for vSphere Auto Deploy	73

- Managing Auto Deploy with PowerCLI Cmdlets 79
- Provisioning ESXi Systems with vSphere Auto Deploy 83
- Setting Up an Auto Deploy Reference Host 86
- Advanced Management Tasks 92
- Auto Deploy Best Practices and Security Consideration 98
- Troubleshooting Auto Deploy 101
- Auto Deploy Proof of Concept Setup 108
- 6 Using vSphere ESXi Image Builder CLI 123**
  - Understanding Image Builder 123
  - Image Builder Installation and Usage 130
  - Image Builder Common Tasks 131
  - Image Builder Workflows 138
- 7 Setting Up ESXi 145**
  - ESXi Autoconfiguration 145
  - About the Direct Console ESXi Interface 146
  - Set the Password for the Administrator Account 148
  - Configuring the BIOS Boot Settings 149
  - Host Fails to Boot After You Install ESXi in UEFI Mode 150
  - Network Access to Your ESXi Host 150
  - Configure the Network Settings on a Host That Is Not Attached to the Network 151
  - Managing ESXi Remotely 151
  - Configuring Network Settings 152
  - Storage Behavior 156
  - View System Logs 159
  - Configure Syslog on ESXi Hosts 159
  - Enable Lockdown Mode Using the Direct Console 160
  - Enable ESXi Shell and SSH Access with the Direct Console User Interface 161
  - Set the Host Image Profile Acceptance Level 161
  - Reset the System Configuration 162
  - Remove All Custom Packages on ESXi 163
  - Disable Support for Non-ASCII Characters in Virtual Machine File and Directory Names 163
  - Disable ESXi 163
- 8 After You Install and Set Up ESXi 165**
  - Managing the ESXi Host with the vSphere Client and the vSphere Web Client 165
  - Licensing ESXi Hosts 165
- 9 Preparing vCenter Server Databases 169**
  - vCenter Server Database Patch and Configuration Requirements 169
  - Create a 64-Bit DSN 170
  - Configure vCenter Server to Communicate with the Local Database 171
  - About the Bundled Microsoft SQL Server 2008 R2 Express Database Package 171
  - Maintaining a vCenter Server Database 171
  - Configure DB2 Databases 172
  - Configure Microsoft SQL Server Databases 180
  - Configure Oracle Databases 190

<b>10</b>	<b>Before You Install vCenter Server</b>	<b>197</b>
	vCenter Server Prerequisites	197
	Using a User Account for Running vCenter Server	199
	Installing vCenter Server on IPv6 Machines	200
	JDBC URL Formats for the vCenter Server Database	200
	Configure the URLs on a Standalone vCenter Server System	201
	Running the vCenter Server and vSphere Client Installers from a Network Drive	202
	Required Information for Installing vCenter Server	202
	Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail	204
<b>11</b>	<b>Installing vCenter Server</b>	<b>205</b>
	vCenter Server Components and Support Tools	205
	Download the vCenter Server Installer	206
	Install vCenter Server	206
	Install vCenter Server in a Virtual Machine	208
	Download and Deploy the VMware vCenter Server Appliance	209
<b>12</b>	<b>After You Install vCenter Server</b>	<b>211</b>
	Install vCenter Server Components	212
	Creating vCenter Server Linked Mode Groups	220
	Using a License Server to Manage Version 3.5 ESX or ESXi Hosts	226
	VMware vCenter Management Webservices Service Fails to Start	226
	Back Up the Inventory Service Database on Windows	227
	Restore an Inventory Service Database Backup on Windows	227
	Back Up the Inventory Service Database on Linux	228
	Restore an Inventory Service Database Backup on Linux	228
	Update the vCenter Inventory Service URL Configuration	229
	Reset the vCenter Inventory Service Database	229
	<b>Index</b>	<b>231</b>



# About vSphere Installation and Setup

---

*vSphere Installation and Setup* describes how to install new configurations of VMware<sup>®</sup> 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.

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 the *vSphere Installation and Setup*.

Revision	Description
000783-01	<ul style="list-style-type: none"><li>■ Updated the following topics to distinguish correctly between the dbo schema and the db_owner database role:<ul style="list-style-type: none"><li>■ <a href="#">“Set Database Permissions By Manually Creating Database Roles and the VMW Schema,”</a> on page 182</li><li>■ <a href="#">“Set Database Permissions by Using the dbo Schema and the db_owner Database Role,”</a> on page 183</li></ul></li><li>■ Updated entry for Oracle in Table: <a href="#">Table 9-1</a>.</li><li>■ Corrected step 2 of procedure <a href="#">“Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script,”</a> on page 17.</li></ul>
000783-00	Initial release.



# Introduction to vSphere Installation and Setup

---

# 1

vSphere 5.0 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 5.0 Differs from vSphere 4.x,”](#) on page 11
- [“Overview of the vSphere Installation and Setup Process,”](#) on page 13
- [“Options for Installing ESXi,”](#) on page 14
- [“Media Options for Booting the ESXi Installer,”](#) on page 15
- [“Using Remote Management Applications,”](#) on page 26
- [“Required Information for ESXi Installation,”](#) on page 26

## How vSphere 5.0 Differs from vSphere 4.x

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

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

### **Service Console is removed**

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

### **ESXi does not have a graphical installer**

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

### **vSphere Auto Deploy and vSphere ESXi Image Builder CLI**

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

### Changes in the ESXi installation and upgrade process

For complete information on using vSphere Auto Deploy and ESXi Image Builder PowerCLI, see [Chapter 5, “Installing ESXi Using vSphere Auto Deploy,”](#) on page 63 and [Chapter 6, “Using vSphere ESXi Image Builder CLI,”](#) on page 123.

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

---

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

---

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

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

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

---

**NOTE** Partitioning for hosts that are upgraded to ESXi 5.0 differs significantly from partitioning for new installations of ESXi 5.0. See the *vSphere Upgrade* documentation.

---

### VMware vCenter Server Appliance

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

### vSphere Web Client

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

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

ESXi 5.0 uses the same installer for fresh installations and upgrades or migrations. If the installer finds an existing ESX 4.x or ESXi 4.x 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 15. 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 19.
- 4 Install ESXi:
  - [Chapter 3, “Installing ESXi Interactively,”](#) on page 43
  - [Chapter 4, “Installing, Upgrading, or Migrating Hosts Using a Script,”](#) on page 47
  - [Chapter 5, “Installing ESXi Using vSphere Auto Deploy,”](#) on page 63
- 5 Configure ESXi boot and network settings, the direct console, and other settings. See [Chapter 7, “Setting Up ESXi,”](#) on page 145.
- 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 165.
- 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 37, [“Configure Syslog on ESXi Hosts,”](#) on page 159, [“Set Up Syslog from the Host Profiles Interface,”](#) on page 91, and [“Install vSphere Syslog Collector,”](#) on page 217.
- 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 169.
  - b Install 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 205 and [Chapter 12, “After You Install vCenter Server,”](#) on page 211.
  - 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 220.

## 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 43.

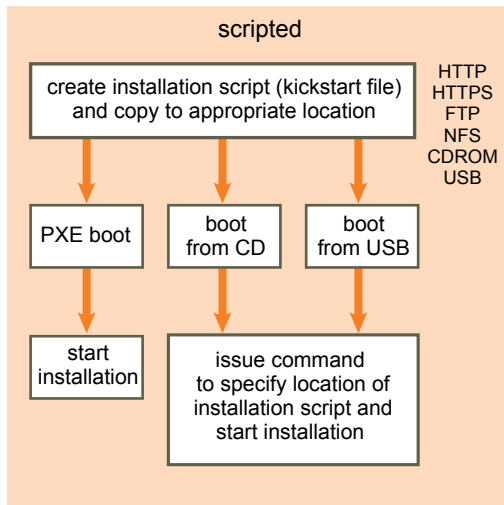
### Scripted ESXi Installation

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 47.

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



### vSphere Auto Deploy ESXi Installation Option

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

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 stores and manages ESXi updates and patching through an image profile, and, optionally, the host configuration through a host profile. You can create image profiles with ESXi Image Builder CLI, and host profiles using the vSphere Client. See [Chapter 6, “Using vSphere ESXi Image Builder CLI,”](#) on page 123 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, vCenter Server uses the Auto Deploy feature to provision the host with the appropriate image and host profile. If the image profile changes, for example, for an update or patch, the administrator can propagate the change to all hosts that are provisioned with Auto Deploy and managed by a vCenter Server system. This ability 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 63.

## 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 123 and [Chapter 5, “Installing ESXi Using vSphere Auto Deploy,”](#) on page 63.

## About ESXi Evaluation and Licensed Modes

After you purchase a host license, VMware provides a serial number that you can use to license vSphere. You can use evaluation mode to access the full ESXi feature set, including features you have not purchased a license for.

For example, in evaluation mode, you can use vMotion, HA, DRS, and other features, even if you have not licensed those features.

The installable version of ESXi is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal USB device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host, even if you start in licensed mode rather than evaluation mode. Any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. To take full advantage of the 60-day evaluation period, you should convert to evaluation mode as soon as possible after you first power on the host. See [“Convert an ESXi Host to Evaluation Mode,”](#) on page 166.

For information about licensing the host, see the *vCenter Server and Host Management*.

## 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 16.
- Boot from a USB flash drive. See [“Format a USB Flash Drive to Boot the ESXi Installation or Upgrade,”](#) on page 16.
- PXE boot from the network. [“PXE Booting the ESXi Installer,”](#) on page 19

- Boot from a remote location using a remote management application. See “Using Remote Management Applications,” on page 26

## 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 18.

### Procedure

- 1 Download the ISO image for ESXi from the VMware download page at <http://www.vmware.com/download/>.
- 2 Burn the ISO image to a CD or DVD.

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

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

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

---

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

---

### Prerequisites

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

### Procedure

- 1 If your USB flash drive is not detected as `/dev/sdb`, or you are not sure how your USB flash drive is detected, determine how it is detected.
  - a In a terminal window, run the following command.
 

```
tail -f /var/log/messages
```

This command displays current log messages in the terminal window.
  - b Plug in your USB flash drive.
 

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

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

In this example, “[sdb]” identifies the USB device. If your device is identified differently, use that identification, without the brackets, in place of `sdb`, in this procedure.
- 2 Create a partition table on the USB flash device.
 

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

  - a Type `d` to delete partitions until they are all deleted.
  - b Type `n` to create primary partition 1 that extends over the entire disk.
  - c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as `c`.



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

e Type **p** to print the partition table.

The result should be similar to the following text:

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

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

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

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

4 Run the following commands.

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

5 Mount the USB flash drive.

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

6 Mount the ESXi installer ISO image.

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

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

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

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

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

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

10 Unmount the USB flash drive.

```
umount /usbdisk
```

11 Unmount the installer ISO image.

```
umount /esxi_cdrom
```

The USB flash drive can now boot the ESXi installer.

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

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

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

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

---

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

---

### Prerequisites

- Linux machine

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

### Procedure

- 1 Attach the USB flash drive to a Linux machine that has access to the installation or upgrade script.
- 2 Create a partition table.

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

- a Type `d` to delete partitions until they are all deleted.
- b Type `n` to create primary partition 1 that extends over the entire disk.
- c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as `c`.
- d Type `p` to print the partition table.

The result should be similar to the following text:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *           1         243       1951866   c   W95 FAT32 (LBA)
```

- e Type `w` to write the partition table and quit.
- 3 Format the USB flash drive with the Fat32 file system.

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

- 4 Mount the USB flash drive.

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

- 5 Copy the ESXi installation script to the USB flash drive.

```
cp ks.cfg /usbdisk
```

- 6 Unmount the USB flash drive.

The USB flash drive contains the installation or upgrade script for ESXi.

### What to do next

When you boot the ESXi installer, point to the location of the USB flash drive for the installation or upgrade script. See [“Enter Boot Options to Start an Installation or Upgrade Script,”](#) on page 48 and [“About PXE Configuration Files,”](#) on page 22.

## 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 50 and [“About the boot.cfg File,”](#) on page 58.

### 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_custom.cfg /esxi_cdrom
```

- 5 (Optional) Modify the `boot.cfg` file to specify the location of the installation or upgrade script using the `kernelopt` option.

This step makes the installation or upgrade completely automatic, without the need to specify the kickstart file during the installation or upgrade.

- 6 Recreate the ISO image:

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot  
-boot-load-size 4 -boot-info-table /esxi_cdrom
```

The ISO image now includes your custom installation or upgrade script.

### What to do next

Install ESXi from the ISO image.

## PXE Booting the ESXi Installer

You use the preboot execution environment (PXE) to boot a host and launch the ESXi installer from a network interface.

ESXi 5.0 is distributed in an ISO format that is designed to install to flash memory or to a local hard drive. You can extract the files and boot using PXE.

PXE uses DHCP and Trivial File Transfer Protocol (TFTP) to boot an operating system over a network.

PXE booting requires some network infrastructure and a machine with a PXE-capable network adapter. Most machines that are capable of running ESXi have network adapters that are able to PXE boot.

---

**NOTE** Ensure that the Auto Deploy server has an IPv4 address. PXE booting is supported only with IPv4.

---

### About the TFTP Server, PXELINUX, and gPXE

Trivial File Transfer Protocol (TFTP) is similar to the FTP service, and is typically used only for network booting systems or loading firmware on network devices such as routers.

Most Linux distributions include a copy of the `tftpd-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.

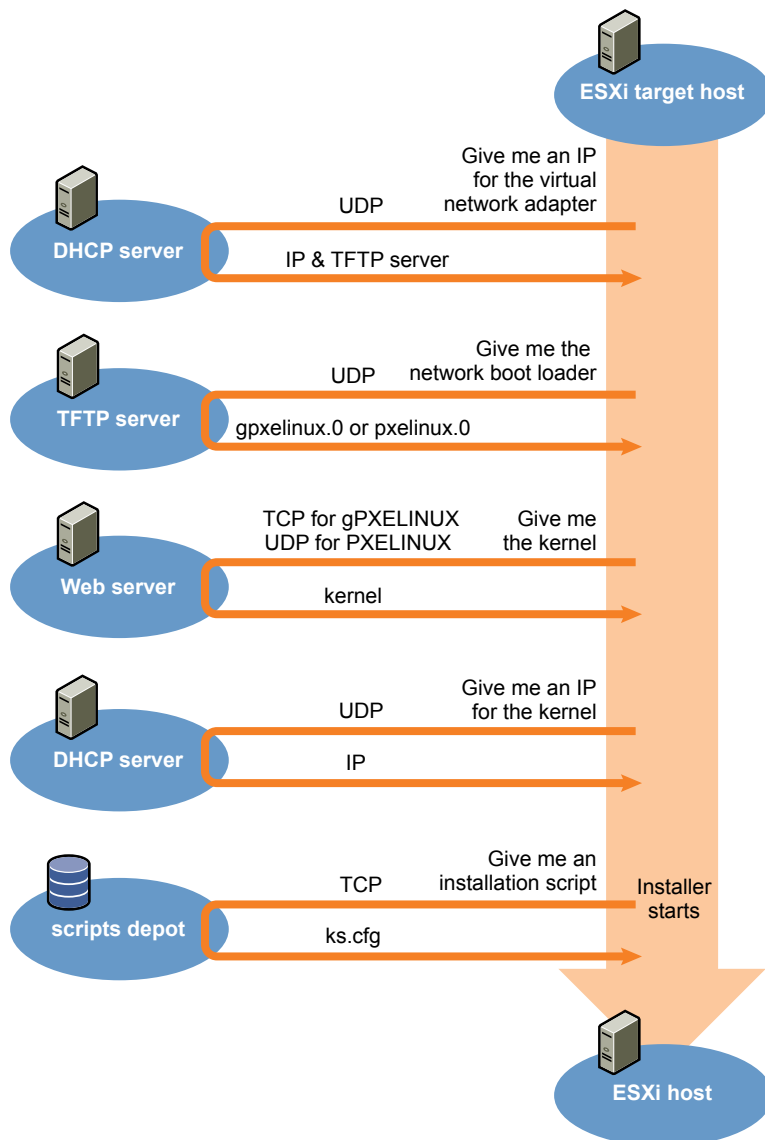
If you do not use gPXE, you might experience problems while booting the ESXi installer on a heavily loaded network. TFTP is sometimes unreliable for transferring large amounts of data. If you use PXELINUX without gPXE, the `pxelinux.0` binary file, the configuration file, the kernel, and other files 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 gppe;
option gppe-encap-opts code 175 = encapsulate gppe;
option gppe.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 gppe.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 58

### 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 50 and [“About the boot.cfg File,”](#) on page 58

### 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 19.

- DHCP server configured for PXE booting. See “[Sample DHCP Configuration](#),” on page 21.
- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.0. See the Hardware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php>.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See “[About Installation and Upgrade Scripts](#),” on page 50.
- Network adapter with PXE support on the target ESXi host
- IPv4 networking. IPv6 is not supported for PXE booting.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

### Procedure

- 1 Create the `/tftpboot/pxelinux.cfg` directory on your TFTP server.
- 2 On the Linux machine, install PXELINUX.  
  
PXELINUX is included in the SYSLINUX package. Extract the files, locate the `pxelinux.0` file and copy it to the `/tftpboot` directory on your TFTP server.
- 3 Configure the DHCP server to send the following information to each client host:
  - The name or IP address of your TFTP server.
  - The name of your initial boot file. This is `pxelinux.0`.
- 4 Copy the contents of the ESXi installer image to the `/var/lib/tftpboot` directory on the TFTP server.
- 5 (Optional) For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option on the line following the kernel command, to specify the location of the installation script.

Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory containing the `ks.cfg` file.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 Create a PXE configuration file.  
  
This file defines how the host boots when no operating system is present. The PXE configuration file references the boot files. Use the following code as a model, where `XXXXXX` is the build number of the ESXi installer image.

```
DEFAULT menu.c32
MENU TITLE ESXi-5.0.0-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-5.0.0-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 Name the file with the MAC address of the target host machine: `01-mac_address_of_target_ESXi_host`.  
  
For example, `01-23-45-67-89-0a-bc`.

- 8 Save the PXE configuration file in `/tftpboot/pxelinux.cfg` on the TFTP server.
- 9 Boot the machine with the network adapter.

## PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File

You can PXE boot the ESXi installer using PXELINUX, and use the `isolinux.cfg` file as the PXE configuration file.

See also [“About Installation and Upgrade Scripts,”](#) on page 50 and [“About the boot.cfg File,”](#) on page 58

### 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 19.
- DHCP server configured for PXE booting. See [“Sample DHCP Configuration,”](#) on page 21.
- PXELINUX
- Server with a hardware configuration that is supported with ESXi 5.0. See the *Hardware Compatibility Guide* at <http://www.vmware.com/resources/compatibility/search.php>.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See [“About Installation and Upgrade Scripts,”](#) on page 50.
- 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 `/tftboot/pxelinux.cfg` directory.

The `isolinux.cfg` file contains the following code, where `XXXXXX` is the build number of the ESXi installer image:

```
DEFAULT menu.c32
MENU TITLE ESXi-5.0.0-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-5.0.0-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 Rename the `isolinux.cfg` file with the MAC address of the target host machine: `01-mac_address_of_target_ESXi_host`. For example, `01-23-45-67-89-0a-bc`
- 8 Boot the machine with the network adapter.

## PXE Boot the ESXi Installer Using gPXE

You can PXE boot the ESXi installer using gPXE.

See also [“About Installation and Upgrade Scripts,”](#) on page 50 and [“About the boot.cfg File,”](#) on page 58

### 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 21.
- Server with a hardware configuration that is supported with ESXi 5.0. See the Hardware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php>.
- gPXELINUX
- (Optional) ESXi installation script. See [“About Installation and Upgrade Scripts,”](#) on page 50.

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 dhcp is not set)
kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

## Using Remote Management Applications

Remote management applications allow you to install ESXi on servers that are in remote locations.

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see [“Supported Remote Management Server Models and Minimum Firmware Versions,”](#) on page 41. 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	

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

Information	Required or Optional	Default	Comments
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 <a href="#">“Installing ESXi on a Drive with an Existing ESX or ESXi Installation or VMFS Datastore,”</a> on page 13.
Root password	Optional	None	The root password must contain between 6 and 64 characters.



# System Requirements

---

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 73.

This chapter includes the following topics:

- “[ESXi Hardware Requirements](#),” on page 29
- “[ESXi Support for 64-Bit Guest Operating Systems](#),” on page 32
- “[vCenter Server and vSphere Client Hardware Requirements](#),” on page 33
- “[vCenter Server Software Requirements](#),” on page 36
- “[vSphere Client and vSphere Web Client Software Requirements](#),” on page 37
- “[Providing Sufficient Space for System Logging](#),” on page 37
- “[Required Ports for vCenter Server](#),” on page 38
- “[Required Ports for the vCenter Server Appliance](#),” on page 39
- “[Conflict Between vCenter Server and IIS for Port 80](#),” on page 40
- “[DNS Requirements for vSphere](#),” on page 40
- “[Supported Remote Management Server Models and Minimum Firmware Versions](#),” on page 41

## ESXi Hardware Requirements

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

### Hardware and System Resources

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

- Supported server platform. For a list of supported platforms, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.
- ESXi 5.0 will install and run only on servers with 64-bit x86 CPUs.
- ESXi 5.0 requires a host machine with at least two cores.
- ESXi 5.0 supports only LAHF and SAHF CPU instructions.
- ESXi supports a broad range of x64 multicore processors. For a complete list of supported processors, see the VMware compatibility guide at <http://www.vmware.com/resources/compatibility>.

- ESXi requires a minimum of 2GB of physical RAM. VMware recommends 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.
- One or more Gigabit or 10Gb Ethernet controllers. For a list of supported network adapter models, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.
- Any combination of one or more of the following controllers:
  - Basic SCSI controllers. Adaptec Ultra-160 or Ultra-320, LSI Logic Fusion-MPT, or most NCR/Symbios SCSI.
  - RAID controllers. Dell PERC (Adaptec RAID or LSI MegaRAID), HP Smart Array RAID, or IBM (Adaptec) ServeRAID controllers.
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks will be considered remote, not local. These disks will not be used as a scratch partition by default because they are seen as remote.

---

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

---

## Storage Systems

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

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

Supported SAS controllers include:

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

Supported on-board SATA include:

- Intel ICH9
- NVIDIA MCP55
- ServerWorks HT1000

---

**NOTE** ESXi does not support using local, internal SATA drives on the host server to create VMFS datastores that are shared across multiple ESXi hosts.

---

- Serial Attached SCSI (SAS) disk drives. Supported for installing ESXi 5.0 and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI
- USB devices. Supported for installing ESXi 5.0. For a list of supported USB devices, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

## ESXi Booting Requirements

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

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

---

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

---

## Storage Requirements for ESXi 5.0 Installation

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

To reconfigure `/scratch`, see [“Set the Scratch Partition from the vSphere Client,”](#) on page 158.

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	<p>ESXi hosts require more RAM than typical servers. VMware recommends 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host.</p> <p>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.</p> <p>Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines.</p> <p>These calculations do not take into account possible memory savings from using variable overhead memory for each virtual machine. See <i>vSphere Resource Management</i>.</p>
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	<p>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.</p> <p><b>NOTE</b> 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.</p>
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 5.0 drivers. See the <i>Hardware Compatibility Guide</i> at <a href="http://www.vmware.com/resources/compatibility">http://www.vmware.com/resources/compatibility</a> .

## 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 Compatibility Guide* at <http://www.vmware.com/resources/compatibility/search.php>.

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

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



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

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

## vCenter Server and vSphere Client Hardware Requirements

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

### vCenter Server Hardware Requirements

**Table 2-2.** Minimum Hardware Requirements for vCenter Server

vCenter Server Hardware	Requirement
CPU	Two 64-bit CPUs or one 64-bit dual-core processor.
Processor	2.0GHz or faster Intel 64 or AMD 64 processor. The Itanium (IA64) processor is not supported. Processor requirements might be higher if the database runs on the same machine.
Memory	4GB RAM. Memory requirements might be higher if the database runs on the same machine. vCenter Server includes several Java services: VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. When you install vCenter Server, you select the size of your vCenter Server inventory to allocate memory for these services. The inventory size determines the maximum JVM heap settings for the services. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in <a href="#">Table 2-3</a> .
Disk storage	4GB. Disk requirements might be higher if the vCenter Server database runs on the same machine. In vCenter Server 5.0, the default size for vCenter Server logs is 450MB larger than in vCenter Server 4.x. Make sure the disk space allotted to the log folder is sufficient for this increase.
Microsoft SQL Server 2008 R2 Express disk	Up to 2GB free disk space to decompress the installation archive. Approximately 1.5GB of these files are deleted after the installation is complete.
Networking	Gigabit connection recommended.

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

**Table 2-3.** Recommended JVM Heap Settings for vCenter Server

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

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

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

## VMware vCenter Server Appliance Hardware Requirements and Recommendations

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

**Table 2-4.** Hardware Requirements for VMware vCenter Server Appliance

<b>VMware vCenter Server Appliance Hardware</b>	<b>Requirement</b>
Disk storage on the host machine	At least 7GB, and a maximum of 80GB
Memory in the VMware vCenter Server Appliance	<ul style="list-style-type: none"> <li>■ Very small inventory (10 or fewer hosts, 100 or fewer virtual machines): at least 4GB.</li> <li>■ Small inventory (10-100 hosts or 100-1000 virtual machines): at least 8GB.</li> <li>■ Medium inventory (100-400 hosts or 1000-4000 virtual machines): at least 13GB.</li> <li>■ Large inventory (More than 400 hosts or 4000 virtual machines): at least 17GB.</li> </ul>

**Table 2-5.** Recommended JVM Heap Settings for VMware vCenter Server Appliance

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

## vSphere Client Hardware Requirements and Recommendations

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

**Table 2-6.** vSphere Client Minimum Hardware Requirements and Recommendations

vSphere Client Hardware	Requirements and Recommendations
CPU	1 CPU
Processor	500MHz or faster Intel or AMD processor (1GHz recommended)
Memory	500MB (1GB recommended)
Disk Storage	<p>1.5GB free disk space for a complete installation, which includes the following components:</p> <ul style="list-style-type: none"> <li>■ Microsoft .NET 2.0 SP2</li> <li>■ Microsoft .NET 3.0 SP2</li> <li>■ Microsoft .NET 3.5 SP1</li> <li>■ Microsoft Visual J#</li> </ul> <p>Remove any previously installed versions of Microsoft Visual J# on the system where you are installing the vSphere Client.</p> <ul style="list-style-type: none"> <li>■ vSphere Client</li> </ul> <p>If you do not have any of these components already installed, you must have 400MB free on the drive that has the %temp% directory.</p> <p>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.</p>
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 2-7.** Medium Deployment of Up to 50 Hosts and 500 Powered-On Virtual Machines

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

**Table 2-8.** Large Deployment of Up to 300 Hosts and 3,000 Powered-On Virtual Machines

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

**Table 2-9.** Extra-Large Deployment of Up to 1,000 Hosts and 10,000 Powered-On Virtual Machines

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

## vSphere Web Client Hardware Requirements

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

**Table 2-10.** Hardware Requirements for the vSphere Web Client Server Component

vSphere Web Client Server Hardware	Requirement
Memory	At least 2GB: 1GB for the Java heap, and 1GB for <ul style="list-style-type: none"> <li>■ The resident code</li> <li>■ The stack for Java threads</li> <li>■ Global/bss segments for the Java process</li> </ul>
CPU	2.00 GHz processor with 4 cores

## Requirements for Installation of vCenter Server on a Custom Drive

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

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

## vCenter Server Software Requirements

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

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

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

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

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

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

## vSphere Client and vSphere Web Client Software Requirements

Make sure that your operating system supports the vSphere Client.

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

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

The following browsers are supported for the vSphere Web Client:

- Microsoft Internet Explorer 7 and 8
- Mozilla Firefox 3.6

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

## Providing Sufficient Space for System Logging

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

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

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

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

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

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

**Table 2-11.** Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs.

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

For information about setting up a remote log server, see “Configure Syslog on ESXi Hosts,” on page 159, “Set Up Syslog from the Host Profiles Interface,” on page 91, and “Install vSphere Syslog Collector,” on page 217.

## 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 39.

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 2-12.** Ports Required for Communication Between Components

Port	Description
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use <code>http://server</code> instead of <code>https://server</code> . 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 <a href="#">“Conflict Between vCenter Server and IIS for Port 80,”</a> on page 40.
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 <code>ip-address:port</code> when you log in to the vCenter Server system.
636	For vCenter Server Linked Mode, this is the SSL port of the local instance. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the SSL service on any port from 1025 through 65535.
902	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts.
903	Port 903 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this ports to display virtual machine consoles.
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
60099	Web Service change service notification port
10443	vCenter Inventory Service HTTPS

**Table 2-12.** Ports Required for Communication Between Components (Continued)

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

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

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

## Required Ports for the vCenter Server Appliance

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

For information about ports required for vCenter Server on Windows, see [“Required Ports for vCenter Server,”](#) on page 38.

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 2-13](#). For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

**Table 2-13.** Ports Required for the vCenter Server Appliance

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

**Table 2-13.** Ports Required for the vCenter Server Appliance (Continued)

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

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

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

## Conflict Between vCenter Server and IIS for Port 80

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

### Problem

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

### Cause

If you do not have IIS installed when you install vSphere Authentication Proxy, the installer prompts you to install IIS. Because IIS uses port 80, which is the default port for vCenter Server direct HTTP connections, vCenter Server fails to restart after the installation of vSphere Authentication Proxy is complete. See [“Required Ports for vCenter Server,”](#) on page 38.

### Solution

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

Option	Description
<b>If you installed IIS before installing vCenter Server</b>	Change the port for vCenter Server direct HTTP connections from 80 to another value.
<b>If you installed vCenter Server before installing IIS</b>	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 2-14.** Supported Remote Management Server Models and Firmware Versions

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



# Installing ESXi Interactively

---

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,”](#) on page 43
- [“Install ESXi on a Software iSCSI Disk,”](#) on page 45

## Install ESXi Interactively

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

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

### Prerequisites

- You must have the ESXi 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 16
  - On a USB flash drive. See [“Format a USB Flash Drive to Boot the ESXi Installation or Upgrade,”](#) on page 16.

---

**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 19.

---

- 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 26.
- 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 26.

### 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 F11 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 150

---

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 165.

**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 reenale 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, reenale the option to boot to the iSCSI target, so the system will boot from the LUN you installed 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,”](#) on page 47
- [“Enter Boot Options to Start an Installation or Upgrade Script,”](#) on page 48
- [“About Installation and Upgrade Scripts,”](#) on page 50
- [“Install, Upgrade, or Migrate ESXi from a CD or DVD Using a Script,”](#) on page 59
- [“Install, Upgrade, or Migrate ESXi from a USB Flash Drive Using a Script,”](#) on page 60
- [“Performing a Scripted Installation or Upgrade of ESXi by PXE Booting the Installer,”](#) on page 61

## 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 51.

## Enter Boot Options to Start an Installation or Upgrade Script

You can start an installation or upgrade script by typing boot command-line options at the boot command line.

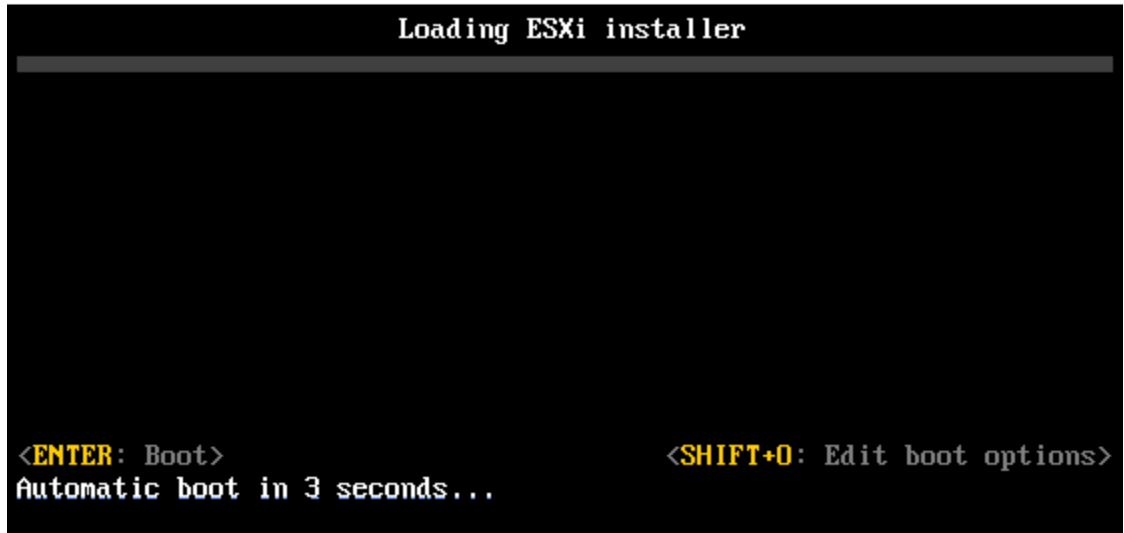
At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See [“About the boot.cfg File,”](#) on page 58 and [“PXE Booting the ESXi Installer,”](#) on page 19.

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 49.

### 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
<code>B00TIF=<i>hwtype</i>-<i>MAC</i> <i>address</i></code>	Similar to the <code>netdevice</code> option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the <a href="http://syslinux.zytor.com">syslinux.zytor.com</a> site.
<code>gateway=<i>ip</i> <i>address</i></code>	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
<code>ip=<i>ip</i> <i>address</i></code>	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 <a href="http://syslinux.zytor.com">syslinux.zytor.com</a> site.
<code>ks=<i>cdrom</i>:/<i>path</i></code>	Performs a scripted installation with the script at <i>path</i> , 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.
<code>ks=<i>file</i>:/<i>path</i></code>	Performs a scripted installation with the script at <i>path</i> .
<code>ks=<i>protocol</i>:/<i>serverpath</i></code>	Performs a scripted installation with a script located on the network at the given URL. <i>protocol</i> can be <code>http</code> , <code>https</code> , <code>ftp</code> , or <code>nfs</code> . The format of an NFS URL is specified in RFC 2224.
<code>ks=<i>usb</i></code>	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named <code>ks.cfg</code> . The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the <code>ks.cfg</code> file is found. Only FAT16 and FAT32 file systems are supported.
<code>ks=<i>usb</i>:/<i>path</i></code>	Performs a scripted installation with the script file at the specified path, which resides on USB.
<code>ksdevice=<i>device</i></code>	Tries to use a network adapter <i>device</i> when looking for an installation script and installation media. Specify as a MAC address, for example, <code>00:50:56:C0:00:01</code> . This location can also be a <code>vmnicNN</code> 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.
<code>nameserver=<i>ip</i> <i>address</i></code>	Specifies a domain name server to be used for downloading the installation script and installation media.
<code>netdevice=<i>device</i></code>	Tries to use a network adapter <i>device</i> when looking for an installation script and installation media. Specify as a MAC address, for example, <code>00:50:56:C0:00:01</code> . This location can also be a <code>vmnicNN</code> 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.
<code>netmask=<i>subnet</i> <i>mask</i></code>	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
<code>vlanid=<i>vlanid</i></code>	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 48.

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 18.
- USB Flash drive. See [“Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script,”](#) on page 17.
- A location accessible with the following protocols: NFS, HTTP, HTTPS, FTP

## Path to the Installation or Upgrade Script

You can specify the path to an installation or upgrade script.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` is the path to the ESXi installation script, where `XXX.XXX.XXX.XXX` is the IP address of the machine where the script resides. See [“About Installation and Upgrade Scripts,”](#) on page 50.

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 48.

## 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.

<b>--drives=</b>	Remove partitions on the specified drives.
<b>--alldrives</b>	Ignores the <code>--drives=</code> requirement and allows clearing of partitions on every drive.
<b>--ignoredrives=</b>	Removes partitions on all drives except those specified. Required unless the <code>--drives=</code> or <code>--alldrives</code> flag is specified.
<b>--overwritevmfs</b>	Permits overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.
<b>--firstdisk= disk-type1 [disk-type2,...]</b>	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: <ol style="list-style-type: none"> <li>1 Locally attached storage (<code>local</code>)</li> <li>2 Network storage (<code>remote</code>)</li> <li>3 USB disks (<code>usb</code>)</li> </ol>

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=vm1.000000034211234`
- vmkLUN UID: `--disk=vmkLUN_UID`

For accepted disk name formats, see [“Disk Device Names,”](#) on page 58.

**--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.

**--novmfsdisk**

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=vm1.000000034211234`
- vmkLUN UID: `--disk=vmkLUN_UID`

For accepted disk name formats, see [“Disk Device Names,”](#) on page 58.

**--firstdisk=  
*disk-type1*,  
[*disk-type2*,...]**

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

- 1 Locally attached storage (*local*)
- 2 Network storage (*remote*)
- 3 USB disks (*usb*)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name `ST3120814A` and any disk that uses the `mptsas` driver rather than a normal local disk, the argument is

`--firstdisk=ST3120814A,mptsas,local`.

**--overwritevmfs**

Install ESXi if a VMFS partition exists on the disk, but no ESX or ESXi installation exists. Unless this option is present, the installer will fail if a VMFS partition exists on the disk, but no ESX or ESXi installation exists.

**--forcemigrate**

If the host contains customizations, such as third-party VIBs or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The `forcemigrate` option overrides the error and forces the upgrade.



**CAUTION** Using the `forcemigrate` option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.

## keyboard (optional)

Sets the keyboard type for the system.

***keyboardType***

Specifies the keyboard map for the selected keyboard type. *keyboardType* must be one of the following types.

- Belgian
- Brazilian
- Croatian

- Czechoslovakian
- Danish
- Default
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- US Dvorak
- Ukranian
- United Kingdom

## network (optional)

Specify a network address for the system.

<b>--bootproto=[dhcp static]</b>	Specify whether to obtain the network settings from DHCP or set them manually.
<b>--device=</b>	Specifies either the MAC address of the network card or the device name, in the form <code>vmnicNN</code> , as in <code>vmnic0</code> . This options refers to the uplink device for the virtual switch.
<b>--ip=</b>	Sets an IP address for the machine to be installed, in the form <code>xxx.xxx.xxx.xxx</code> . Required with the <code>--bootproto=static</code> option and ignored otherwise.
<b>--gateway=</b>	Designates the default gateway as an IP address, in the form <code>xxx.xxx.xxx.xxx</code> . Used with the <code>--bootproto=static</code> option.

<b>--nameserver=</b>	Designates the primary name server as an IP address. Used with the <b>--bootproto=static</b> option. Omit this option if you do not intend to use DNS.  The <b>--nameserver</b> option can accept two IP addresses. For example: <b>--nameserver="10.126.87.104[,10.126.87.120]"</b>
<b>--netmask=</b>	Specifies the subnet mask for the installed system, in the form 255.xxx.xxx.xxx. Used with the <b>--bootproto=static</b> option.
<b>--hostname=</b>	Specifies the host name for the installed system.
<b>--vlanid= <i>vlanid</i></b>	Specifies which VLAN the system is on. Used with either the <b>--bootproto=dhcp</b> or <b>--bootproto=static</b> option. Set to an integer from 1 to 4096.
<b>--addvmportgroup={0 1}</b>	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

<b><i>datastore name</i></b>	Specifies where the partition is to be mounted
<b>--ondisk= or --ondrive=</b>	Specifies the disk or drive where the partition is created.
<b>--firstdisk=</b> <b><i>disk-type1,</i></b> <b><i>[disk-type2,...]</i></b>	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: <ol style="list-style-type: none"> <li>1 Locally attached storage (<b>local</b>)</li> <li>2 Network storage (<b>remote</b>)</li> <li>3 USB disks (<b>usb</b>)</li> </ol> <p>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 <b>esx</b> 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 <b>--firstdisk=ST3120814A,mptsas,local</b>.</p>

### reboot (optional)

Reboots the machine after the scripted installation is complete.

<b>&lt;--noeject&gt;</b>	The CD is not ejected after the installation.
--------------------------	---

## rootpw (required)

Sets the root password for the system.

<b>--iscrypted</b>	Specifies that the password is encrypted.
<b>password</b>	Specifies the password value.

## upgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

<b>--disk= or --drive=</b>	Specifies the disk to partition. In the command <code>--disk=diskname</code> , the <i>diskname</i> can be in any of the forms shown in the following examples: <ul style="list-style-type: none"> <li>■ Path: <code>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</code></li> <li>■ MPX name: <code>--disk=mpx.vmhba1:C0:T0:L0</code></li> <li>■ VML name: <code>--disk=vml.000000034211234</code></li> <li>■ vmkLUN UID: <code>--disk=vmkLUN_UID</code></li> </ul>
----------------------------	--

For accepted disk name formats, see [“Disk Device Names,”](#) on page 58.

<b>--firstdisk= disk-type1, [disk-type2,...]</b>	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: <ol style="list-style-type: none"> <li>1 Locally attached storage (<code>local</code>)</li> <li>2 Network storage (<code>remote</code>)</li> <li>3 USB disks (<code>usb</code>)</li> </ol>
--	---

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`.

<b>--deletecosvmdk</b>	If the system is being upgraded from ESX, remove the directory that contains the old Service Console VMDK file, <code>cos.vmdk</code> , to reclaim unused space in the VMFS datastore.
<b>--forcemigrate</b>	If the host contains customizations, such as third-party VIBs or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The <code>forcemigrate</code> option overrides the error and forces the upgrade.



**CAUTION** Using the `forcemigrate` option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.



**%include or include (optional)**

Specifies another installation script to parse. This command is treated similarly to a multiline command, but takes only one argument.

*filename* For example: %include part.cfg

**%pre (optional)**

Specifies a script to run before the kickstart configuration is evaluated. For example, you can use it to generate files for the kickstart file to include.

**--interpreter** Specifies an interpreter to use. The default is busybox.  
**=*[python|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** Specifies an interpreter to use. The default is busybox.  
**=*[python|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** If true, the installation is considered a success even if the %post script terminated with an error.  
**=*[true|false]***

**%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** Specifies an interpreter to use. The default is busybox.  
**=*[python|busybox]***

---

**NOTE** You cannot check the semantics of the %firstboot script until the system boots for the first time. If the script contains errors, they are not exposed until after the installation is complete.

---

## Differences Between ESXi 4.x and ESXi 5.0 Scripted Installation and Upgrade Commands

Before you perform a scripted ESXi installation or upgrade, if you are familiar with ESXi version 4.x scripted installation, note the differences between ESXi 4.x and ESXi 5.0 scripted installation and upgrade commands.

In ESXi 5.0, because the installation image is loaded directly into the host RAM when the host boots, you do not need to include the location of the installation media in the installation script.

ESXi 5.0 supports scripted upgrades in addition to scripted installation.

Command differences are noted in the following summary.

<b>accepteula OR vmaccepteula</b>	Only in ESXi
<b>autopart</b>	Deprecated and replaced with <code>install</code> , <code>upgrade</code> , or <code>installorupgrade</code> .
<b>auth OR authconfig</b>	Not supported in ESXi 5.0.
<b>bootloader</b>	Not supported in ESXi 5.0.
<b>esxlocation</b>	Deprecated and unused in ESXi.
<b>firewall</b>	Not supported in ESXi 5.0.
<b>firewallport</b>	Not supported in ESXi 5.0.
<b>install, installorupgrade, upgrade</b>	These commands replace the deprecated <code>autopart</code> command. Use one of these command to specify the disk to partition, and the <code>part</code> command to create the vmfs datastore. <code>installorupgrade</code> and <code>upgrade</code> are newly supported in ESXi 5.0.
<b>serialnum OR vmserialnum</b>	Deprecated in ESXi 5.0. You can license the host only after installation. See <a href="#">“Licensing ESXi Hosts,”</a> on page 165
<b>timezone</b>	Not supported in ESXi 5.0.
<b>virtualdisk</b>	Not supported in ESXi 5.0.
<b>zerombr</b>	Not supported in ESXi 5.0.
<b>%firstboot</b>	<code>--level</code> option not supported in ESXi 5.0.
<b>%packages</b>	Not supported in ESXi 5.0.

## Disk Device Names

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

**Table 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 5.0, the MPX and VML disk names change, which might cause the upgrade to fail. To avoid this problem, use Network Address Authority Identifiers (NAA IDs) for the disk device instead of MPX and VML disk names.

## About the boot.cfg File

The boot loader configuration file `boot.cfg` specifies the kernel, the kernel options, and the boot modules that the `mboot.c32` boot loader uses in an ESXi installation.

The `boot.cfg` file is provided in the ESXi installer. You can modify the `kernelopt` line of the `boot.cfg` file to specify the location of an installation script or to pass other boot options.

The boot.cfg file has the following syntax:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

The commands in boot.cfg configure the boot loader.

**Table 4-4.** Commands in boot.cfg .

Command	Description
title=STRING	Sets the boot loader title to <i>STRING</i> .
kernel=FILEPATH	Sets the kernel path to <i>FILEPATH</i> .
kernelopt=STRING	Appends <i>STRING</i> 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 18, [“PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File,”](#) on page 22, [“PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File,”](#) on page 24, and [“PXE Booting the ESXi Installer,”](#) on page 19.

## 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 18.

### Prerequisites

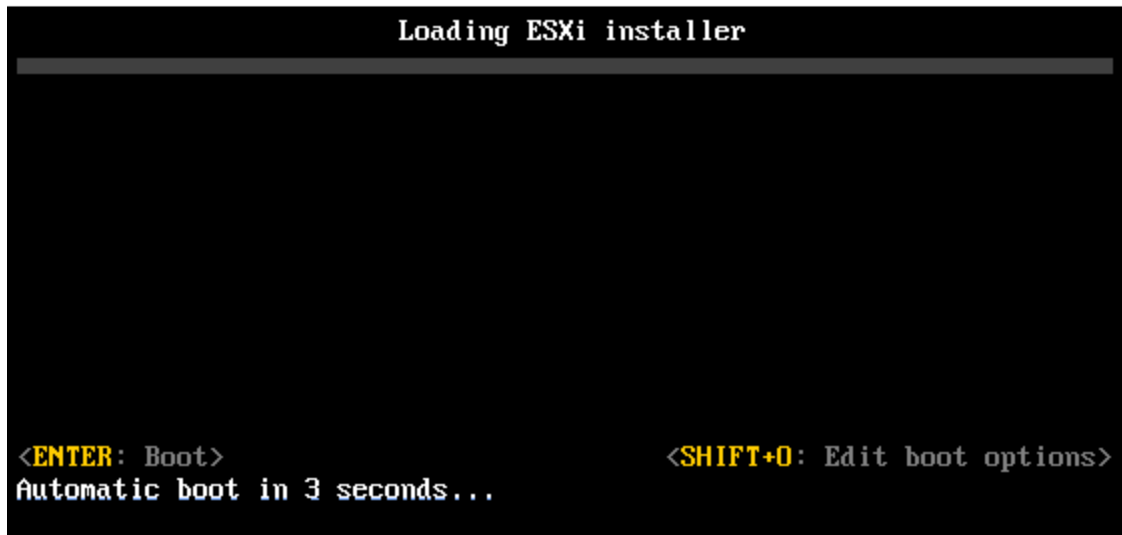
Before you run the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- 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 16.
- 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 50.
- 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 48. For a complete list of boot commands, see [“Boot Options,”](#) on page 49.

### 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 49.

### Prerequisites

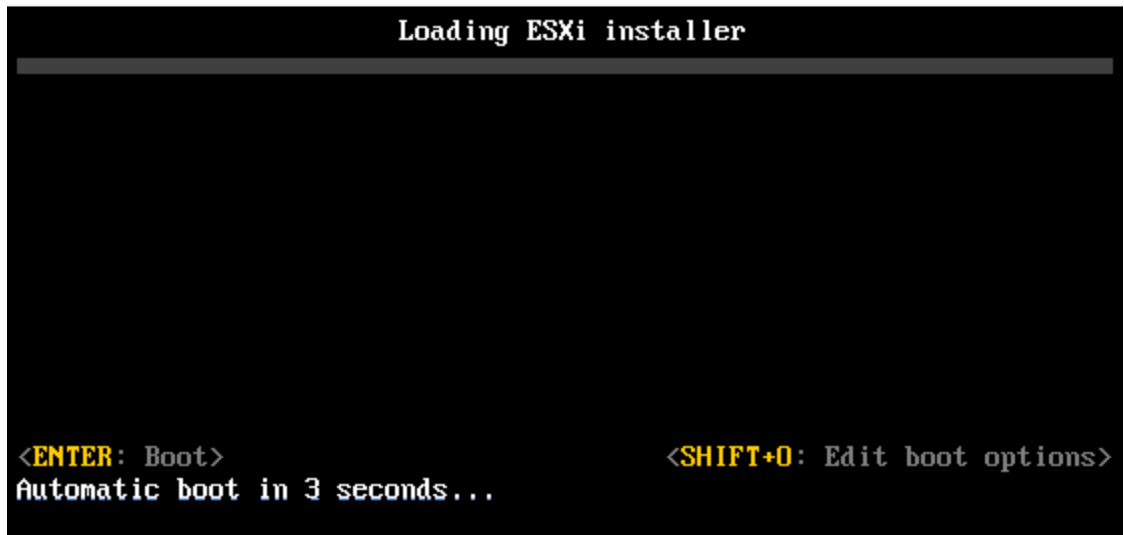
Before running the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- 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 16.
- 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 50.
- 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 48.

### Procedure

- 1 Boot the ESXi installer from the USB flash drive.

- 2 When the ESXi installer window appears, press Shift+O to edit boot options.



- 3 Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

The boot option has the form `ks=`.

- 4 Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

## Performing a Scripted Installation or Upgrade of ESXi by PXE Booting the Installer

ESXi 5.0 provides many options for PXE booting the installer and using an installation or upgrade script.

- For information about setting up a PXE infrastructure, see [“PXE Booting the ESXi Installer,”](#) on page 19.
- For information about creating and locating an installation script, see [“About Installation and Upgrade Scripts,”](#) on page 50.
- 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 24
  - [“PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File,”](#) on page 22
  - [“PXE Boot the ESXi Installer Using gPXE,”](#) on page 25
- 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 63.



# Installing ESXi Using vSphere Auto Deploy

---

# 5

Using the vSphere Auto Deploy feature, you can provision hundreds of physical hosts with ESXi software.

Using Auto Deploy, experienced system administrators can manage large deployments efficiently. Unlike the other installation options, Auto Deploy does not store ESXi configuration or state on the host disk. Instead, state is managed through an image profile and other host attributes are managed through host profiles.

This chapter includes the following topics:

- [“Understanding vSphere Auto Deploy,”](#) on page 63
- [“Auto Deploy Roadmap and Cmdlet Overview,”](#) on page 70
- [“Preparing for vSphere Auto Deploy,”](#) on page 73
- [“Managing Auto Deploy with PowerCLI Cmdlets,”](#) on page 79
- [“Provisioning ESXi Systems with vSphere Auto Deploy,”](#) on page 83
- [“Setting Up an Auto Deploy Reference Host,”](#) on page 86
- [“Advanced Management Tasks,”](#) on page 92
- [“Auto Deploy Best Practices and Security Consideration,”](#) on page 98
- [“Troubleshooting Auto Deploy,”](#) on page 101
- [“Auto Deploy Proof of Concept Setup,”](#) on page 108

## 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 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. When a host boots for the first time, the vCenter Server system creates a corresponding host object and stores the information in the database.

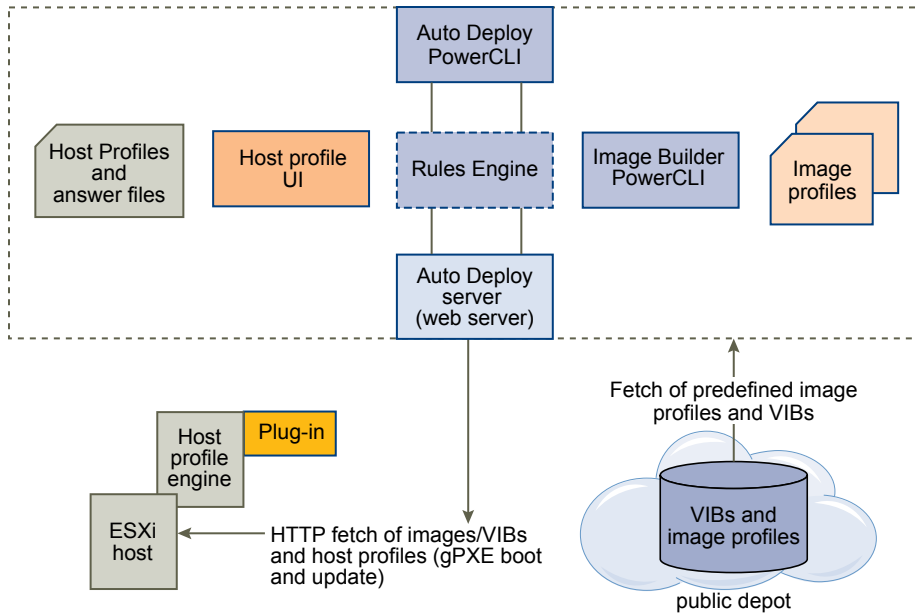
**Table 5-1.** Auto Deploy Stores Information for Deployment

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).	<p>Managed by vCenter Server system by default.</p> <ul style="list-style-type: none"> <li>■ If the virtual machine is in a vSphere HA cluster, deployment works even if the vCenter Server is unavailable because Auto Deploy retains the virtual machine information.</li> <li>■ If the virtual machine is not in a vSphere HA cluster, vCenter Server must be available to supply virtual machine information to Auto Deploy.</li> </ul>
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.	<p>Custom information is stored in an answer file. You can create a host profile that requires user input for certain values.</p> <p>When Auto Deploy applies a host profile that requires an answer to a newly-provisioned host, the host comes up in maintenance mode. You can right-click the host and select <b>Update Answer File</b> to be prompted for the information.</p> <p>The answer file information is stored with the host. Each host has one answer file that can include multiple user input items.</p>

## 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 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 rule 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 export an individual host's host profile and use the host profile to reprovision that host. You can export the host profile of a template host and use the template profile for other hosts.

**Answer files**

Store information that the user provides when host profiles are applied to the host. The answer file might contain an IP address or other information that the user supplied for that host. One answer file can exist for each host. See [“Customizing Hosts with Answer Files,”](#) on page 95.

## 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 rule 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 rule 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 rule 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 vCenter Server has stored in the host object is used. You can use Auto Deploy PowerCLI cmdlets to test and repair rule compliance. When you repair rule compliance for a host, 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.

---

The rule 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 either items or patterns. 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.

You can activate the rules explicitly, however, 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.

## Auto Deploy Boot Process

When you turn on 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 73.

- 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 gPXE boot loader from.
- Ensure that the Auto Deploy server has an IPv4 address. PXE booting is supported only with IPv4.
- 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.
- 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 gPXE file (executable boot loader) and a gPXE configuration file.
- 3 gPXE starts executing.
 

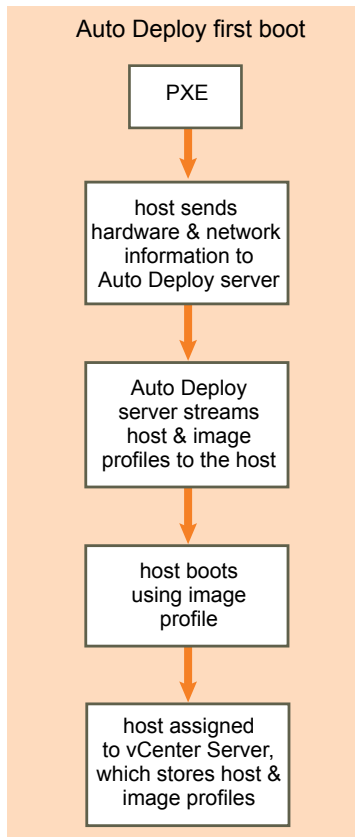
The configuration file instructs the host to make a HTTP boot request to the Auto Deploy server. The HTTP request includes hardware and network information.
- 4 In response, the Auto Deploy server performs these tasks:
  - a Queries the rule engine for information about the host.
  - b Streams the components 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 assigns 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.
  - 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 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,”](#) on page 86.
- 8 If the host is part of a DRS cluster, virtual machines from other hosts might be assigned to the host after the host has successfully been added to the vCenter Server system.

See [“Provision a Host \(First Boot\),”](#) on page 83.

**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. The host is provisioned by the vCenter Server system, which stores information about the image profile and host profile for each host in the database.

The boot process proceeds as follows.

- 1 The administrator reboots the host.
- 2 As the host boots up, Auto Deploy provisions the host with its image profile and host profile, which are stored in vCenter Server.

- 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 server for image profiles and host profiles and the host reboots. However, 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 84.

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,”](#) on page 86.

## Subsequent Boots With Updates

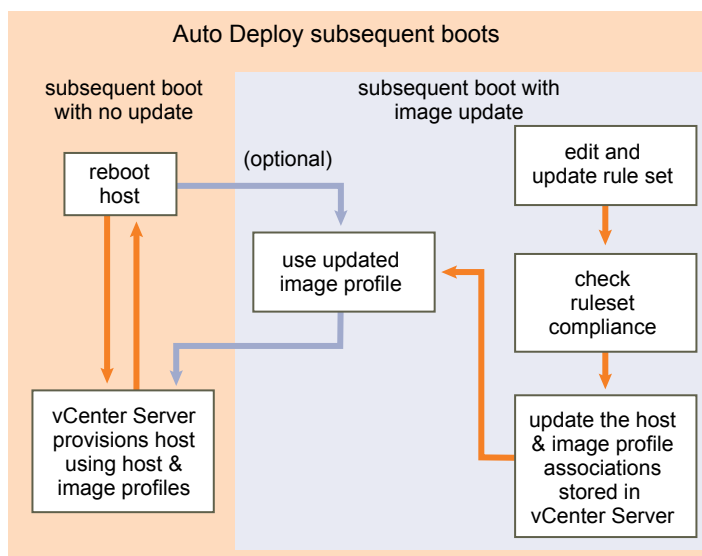
You can change the image profile, host profile, or vCenter Server location for hosts. The process includes changing rules and testing and repairing the host's rule compliance.

- 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 70 for an example.
- 2 The administrator runs the `Test-DeployRulesetCompliance` cmdlet to check whether each host is using the information 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,”](#) on page 86.

See [“Test and Repair Rule Compliance,”](#) on page 82.

**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 108 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. 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. The Auto Deploy server on the vCenter Server appliance is disabled by default. See [“Using Auto Deploy with the VMware vCenter Server Appliance,”](#) on page 93 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 73 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 76 and [“Using Auto Deploy Cmdlets,”](#) on page 76.

- 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.

```
NewDeployRule -Name "testrule" -Item image-profile -AllHosts
```

See [“Assign an Image Profile to Hosts,”](#) on page 79.

---

**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 create an answer file for each host. See [“Use Hosts with Static IP Addresses,”](#) on page 93.

---

- 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 86.
- 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 .

```
CopyDeployRule -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 an answer file has an up-to-date answer file.

Remedy answer file and compliance problems and reboot hosts until all hosts meet the requirements.

Read [“Understanding vSphere Auto Deploy,”](#) on page 63 for an introduction to the boot process, a discussion of differences between first and subsequent boots, and an overview of using answer files.

## 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 76. 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
<code>Get-DeployCommand</code>	Returns a list of Auto Deploy cmdlets.
<code>New-DeployRule</code>	Creates a new rule with the specified items and patterns.
<code>Set-DeployRule</code>	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set.
<code>Get-DeployRule</code>	Retrieves the rules with the specified names.
<code>Copy-DeployRule</code>	Clones and updates an existing rule.
<code>Add-DeployRule</code>	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the <code>NoActivate</code> parameter to add a rule only to the working rule set.
<code>Remove-DeployRule</code>	Removes one or more rules from the working rule set and from the active rule set. Run this command with the <code>-Delete</code> parameter to completely delete the rule.
<code>Set-DeployRuleset</code>	Explicitly sets the list of rules in the working rule set.
<code>Get-DeployRuleset</code>	Retrieves the current working rule set or the current active rule set.
<code>Switch-ActiveDeployRuleset</code>	Activates a rule set so that any new requests are evaluated through the rule set.
<code>Get-VMHostMatchingRules</code>	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.
<code>Test-DeployRulesetCompliance</code>	Checks whether the items associated with a specified host are in compliance with the active rule set.
<code>Repair-DeployRulesetCompliance</code>	Given the output of <code>Test-DeployRulesetCompliance</code> , 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.
<code>Apply-EsxImageProfile</code>	Associates the specified image profile with the specified host.
<code>Get-VMHostImageProfile</code>	Retrieves the image profile in use by a specified host. This cmdlet differs from the <code>Get-EsxImageProfile</code> cmdlet in the Image Builder PowerCLI.



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

Command	Description
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.

## 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 73  
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 76  
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 76  
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 77  
You can use the vSphere 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.



**CAUTION** If you set up Auto Deploy to boot a host, vSphere checks each of the local storage devices on the system for existing partitions. To avoid the possibility of data loss, vSphere does not create partitions under the following conditions:

- A local storage device contains a GPT partition map.
- A local storage device contains an MBR partition table that defines at least one partition.
- Storage is remote.

If hosts have local storage with a partition table that vSphere does not recognize, such as Linux Logical Volume Manager, vSphere overwrites the storage and creates new partitions. To make sure local storage is not considered for partitioning, you can physically disconnect that storage.

### Prerequisites

- Ensure that the hosts you will provision with Auto Deploy meet the hardware requirements for ESXi 5.0. 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 38.

- Do not use VLAN tagged networks at the boot NIC. If you want to specify VLAN IDs, you must make sure that the host can reach the DHCP server when the host starts the boot process. Check with 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 205.

- 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. See [“Auto Deploy Best Practices and Security Consideration,”](#) on page 98.

---

**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 88 and [“Set Up ESXi Dump Collector from the Host Profiles Interface,”](#) on page 90.

See [“Install vSphere ESXi Dump Collector,”](#) on page 216.

- Auto Deploy does not support in a pure IPv6 environment because the PXE boot infrastructure requires IPv4.

## 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
<b>vCenter Server system</b>	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 <a href="#">“Install vSphere Auto Deploy,”</a> on page 218.
<b>Windows system</b>	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 <a href="#">“Install vSphere Auto Deploy,”</a> on page 218.
<b>vCenter Server Appliance</b>	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 <a href="#">“Using Auto Deploy with the VMware vCenter Server Appliance,”</a> on page 93.

- 2 Configure the TFTP server.
  - 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.
- 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 you want to use and the depot in which it is located.  
  
In most cases, you point to an image profile 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 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, it contacts the DHCP server and is directed to the Auto Deploy server, which provisions the host with the image specified in the active rule set.

### What to do next

- Install PowerCLI. See [“Install PowerCLI and Prerequisite Software,”](#) on page 76.
- 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 73.
- Configure the first host your provision to use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for that host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- 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,”](#) on page 95.

## 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 76. 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 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 76.

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

#### Assign license keys with vSphere 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-vmware"
$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 Verify that the host is successfully assigned to the default license XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.
  - a Using a vSphere Client, log in to the vCenter Server system.
  - b Navigate to the **Configuration > License Features** tab for the host and check that the correct license is displayed.

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 76.

#### 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 <b>Add-EsxSoftwareDepot <i>depot_url</i></b> .
ZIP file	a Download the ZIP file to a local file path. b Run <b>Add-EsxSoftwareDepot C:\<i>file_path</i>\my_offline_depot.zip</b> .

- 4 In the depot, find the image profile 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 full 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 gPXE, 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:
* . vendor=VMware, Inc.
* . asset=No Asset Tag
* . domain=
* . serial=VMware-XX XX XX XX XX...
* . uuid=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . hostname=myhost.mycompany.com
* . ipv4=NN.NN.NNN.NNN
* . model=VMware Virtual Platform
* . mac=00:NN:NN:NN:NN:NN
*
*****
```

#### **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 82.
- 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 82.

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 76.



## Procedure

- 1 Run the Connect-VIServer PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

**Connect-VIServer 192.XXX.X.XX**

The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

- 2 In the vSphere Client, select **View > Management > Host Profiles** to display the Host Profiles panel and export the host profile that you want to use from there.
- 3 Find the name of the host profile by running Get-VMhostProfile, passing in the server on which the host profile is located.
- 4 At the PowerCLI prompt, define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the host profile.

**New-DeployRule -Name "testrule2" -Item my\_host\_profile -Pattern "vendor=Acme,Zven",  
"ipv4=192.XXX.1.10-192.XXX.1.20"**

The specified item is assigned to all hosts with the specified attributes. This example specifies a rule named testrule2. The rule assigns the specified host profile my\_host\_profile to all hosts with an IP address inside the specified range and with a manufacturer of Acme or Zven.

- 5 Add the rule to the rule set.

**Add-DeployRule testrule2**

By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the NoActivate parameter, the working rule set does not become the active rule set.

## What to do next

- Upgrade existing hosts to use the new host profile by performing compliance test and repair operations on those hosts. See [“Test and Repair Rule Compliance,”](#) on page 82.
- 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 82.

## 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 76.

## 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 compliance test and repair operations on those hosts. See [“Test and Repair Rule Compliance,”](#) on page 82.
- 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 VMware PowerCLI can access those ESXi hosts.

### Prerequisites

- Install VMware PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Auto Deploy Cmdlets,”](#) on page 76.

## Procedure

- 1 Use PowerCLI to check which Auto Deploy rules are currently available.

**Get-DeployRule**

The system returns the rules and the associated items and patterns.

- 2 Make a change to one of the available rules, for example, you might change the image profile and the name of the rule.

**Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile**

You cannot edit a rule already added to a rule set. Instead, you copy the rule and replace the item or pattern you want to change.

- 3 Verify that the host that you want to test rule set compliance for is accessible.

```
Get-VMHost -Name MyEsxi42
```

- 4 Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

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

- 5 Examine the differences between what is in the rule set and what the host is currently using.

```
$tr.itemlist
```

The system returns a table of current and expected items.

CurrentItem	ExpectedItem
-----	-----
My Profile 25	MyProfileUpdate

- 6 Remediate the host to use the revised rule set the next time you boot the host.

```
Repair-DeployRuleSetCompliance $tr
```

### What to do next

If the rule you changed specified the inventory location, the change takes effect when you repair compliance. For all other changes, boot your host to have Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

## 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, define the image using the Image Builder PowerCLI, and fulfill all other prerequisites before you can provision the host.

#### 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 73).
- 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 79.

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 gPXE 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. In the vSphere Client, check the answer file or reapply the host profile and provide the user input when prompted.

The information is stored in an answer file that is associated with the host.

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 84.

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 82.

## Reprovisioning Hosts

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image or a different host profile.

A first boot using Auto Deploy requires that you set up your environment and add rules to the rule set. See [“Preparing for vSphere Auto Deploy,”](#) on page 73.

The following reprovisioning operations are available.

- Simple reboot.
- Reboot of hosts for which the user answered questions during the boot operation.
- Reprovision with a different image profile.
- Reprovision with a different host profile.

### Reprovision Hosts with Simple Reboot Operations

A simple reboot of a host that is provisioned with Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, and vCenter Server location.

Setup includes DHCP server setup, writing rules, and making an image available to the Auto Deploy infrastructure.

#### Prerequisites

Make sure the setup you performed during the first boot operation is in place.

#### Procedure

- 1 Check that the image profile and host profile for the host are still available, and that the host has the identifying information (asset tag, IP address) it had during previous boot operations.
- 2 Place the host in maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

- 3 In the vSphere Client, right-click the host and choose **Reboot**.

The host shuts down. When the host reboots, it uses the image profile that the Auto Deploy server provides. The Auto Deploy server also applies the host profile stored on the vCenter Server system.

## Reprovision a Host with a New Image Profile

You can reprovision the host with a new image profile, host profile, or vCenter Server location by changing the rule for the host and performing a test and repair operation.

Several options for reprovisioning hosts exist.

- If the VIBs that you want to use support live update, you can use an `esxcli software vib` command. In that case, you must also update the rule set to use an image profile that includes the new VIBs upon reboot.
- During testing, you can to apply an image profile to an individual host with the `Apply-ESXImageProfile` cmdlet and reboot the host so the change takes effect. The `Apply-ESXImageProfile` cmdlet updates the association between the host and the image profile but does not install VIBs on the host.
- In all other cases, use this procedure.

### Prerequisites

- Create the image profile you want to boot the host with. Use the Image Builder PowerCLI, discussed in [Chapter 6, “Using vSphere ESXi Image Builder CLI,”](#) on page 123.
- 
- 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 <code>Add-ESXSoftwareDepot <i>depot_url</i></code> .
ZIP file	<ol style="list-style-type: none"> <li>a Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine.</li> <li>b Run <code>Add-ESXSoftwareDepot C:\file_path\my_offline_depot.zip</code>.</li> </ol>

- 4 Run `Copy-DeployRule` and specify the `ReplaceItem` parameter to change the rule that assigns an image profile to hosts.

The following cmdlet replaces the current image profile that the rule assigns to the host with the `my_new_imageprofile` profile. After the cmdlet completes, `myrule` assigns the new image profile to hosts. The old version of `myrule` is renamed and hidden.

**Copy-DeployRule myrule -ReplaceItem my\_new\_imageprofile**

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

See [“Test and Repair Rule Compliance,”](#) on page 82.

When you reboot hosts after compliance repair, Auto Deploy provisions the hosts with the new image profile.

## Applying a Host Profile to Prompt for User Input

If a host required user input during a previous boot, the answers are saved with the vCenter Server in an answer file. If you want to prompt the user for new information, you reapply the host profile.

### Prerequisites

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

### Procedure

- 1 Place the host in maintenance mode. Migrate all virtual machines to different hosts, and place the host into maintenance mode.

Host Type	Action
<b>Host is part of a DRS cluster</b>	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
<b>Host is not part of a DRS cluster</b>	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

- 2 In the vSphere Client, choose **Host Profiles > Apply Profile** and choose the host profile that requires user input when prompted.
- 3 When prompted, provide the user input.

You can now direct the host to exit maintenance mode.

The user input information is saved in an answer file. The next time you boot, the answer file information is applied to the host. One answer file per host is available.

## 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.

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 or the vSphere Client.

### Syslog Server Setup

All ESXi hosts run a syslog service (`vm syslogd`), 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 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 88. 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.

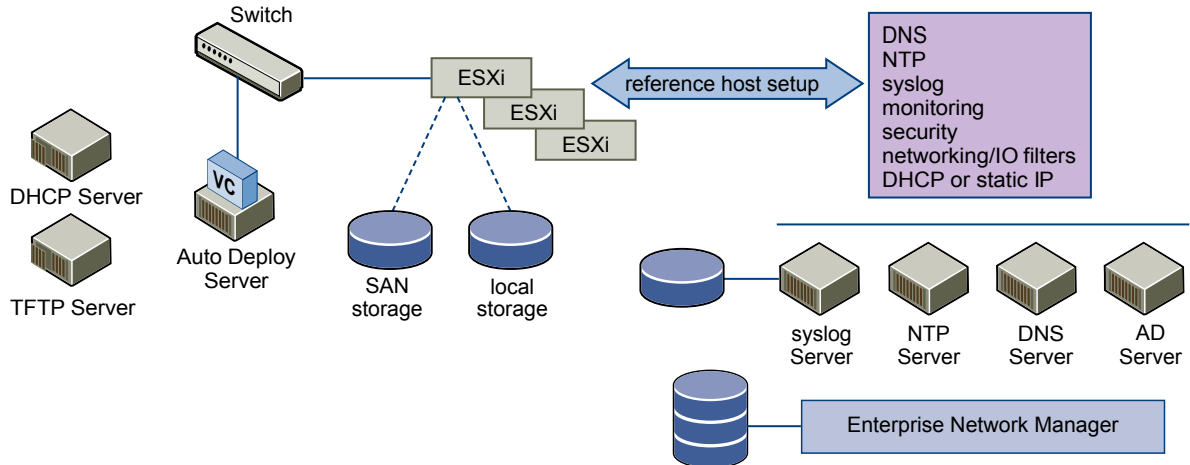
### Security Setup

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. 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 88 explains how to perform this setup.

## Configuring an Auto Deploy Reference Host

vSphere allows you to configure a reference host by using 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 Client

The vSphere Client supports setup of networking, storage, security, and most other aspects of an ESXi host. You can completely set up your environment and export the host profile 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 `vicfg-route` (set up the default route). See [“Configure ESXi Dump Collector with ESXCLI,”](#) on page 88.

### Host Profiles Interface

You can either set up a host with vSphere Client or vCLI and save the host profile for that host, or you can configure the host profiles directly with the Host Profiles interface in the vSphere Client. See [“Configure Host Profiles for an Auto Deploy Reference Host,”](#) on page 89.

## 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 get
```

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 80).
- 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 82.
- Turn on unprovisioned hosts to provision them with the new host profile.

## Configure Host Profiles for an Auto Deploy Reference Host

You can set up host profiles in a reference host and apply those host profile settings to all other hosts provisioned 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

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
<b>ESXi Dump Collector</b>	Set up ESXi Dump Collector with the <code>esxcli system coredump</code> command and save the host profile (best practice), or configure the host profile directly.
<b>Syslog</b>	Set up syslog for the host with the <code>esxcli system syslog</code> command. Save the host profile (best practice) or configure the host profile directly. See <a href="#">“Set Up Syslog from the Host Profiles Interface,”</a> on page 91.

Policy	Description
<b>NTP</b>	Use the <code>vicfg-ntp</code> 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. <ol style="list-style-type: none"> <li>In the vSphere Client, select the <b>Configuration</b> tab and click <b>Time Configuration</b> in the Software panel.</li> <li>Click <b>Properties</b>, click the NTP Client Enabled check box and click <b>Options</b>.</li> <li>Select the <b>Start and stop with host</b> button.</li> </ol>
<b>Security</b>	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.
<b>Networking and Storage</b>	Set up the Networking and Storage policies for the reference host with the vSphere Client or vCLI command.

- 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 80), and perform a test and repair compliance operation.

## Set Up ESXi Dump Collector from the Host Profiles Interface

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 88). In some situations, setting up ESXi Dump Collector from the Host Profiles interface is an alternative.

### Prerequisites

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

### Procedure

- Select **Network Configuration**.
- Select **Network Coredump Settings** and click **Edit**.
- Specify the server port and IP address and the host NIC to use and click the check box to enable ESXi Dump Collector.
- 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 80).
- 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 82.
- Turn on unprovisioned hosts to provision them with the new host profile.

## Set Up Syslog from the Host Profiles Interface

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 For a new profile, click **Create Profile**, or right-click a profile you want to modify and select **Edit Profile**.
- 4 In the Edit Profile dialog, set up the syslog server host profile.
  - If you configure a remote syslog server with the vSphere Client or the `esxcli system syslog` command before you edit host profiles, you can change the remote server and all other syslog options.
    - a Select **Advanced configuration option**.
    - b Select the syslog server settings that you want to use for the hosts provisioned with Auto Deploy.
  - If you do not configure a remote syslog server before you edit host profiles, you must add an advanced option.
    - 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.
- 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 80).
- 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 82.
- 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 80).
- 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 82.
- Turn on unprovisioned hosts to provision them with the new host profile.

## 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 reregister Auto Deploy if the vCenter Server IP address changes.

**Procedure**

- ◆ Perform the reregistration task depending on the operating system.

Operating system	Task
<b>Windows</b>	<p>a Edit the setup file located at <code>c:\ProgramData\VMware\VMware vCenter Auto Deploy\vmconfig-autodeploy.xml</code> and specify the new IP address.</p> <p>You do not have to edit the file if you reregister for other reasons than a new IP address.</p> <p>b Run the <code>autodeploy-register.exe</code> command-line tool, specifying all required options.</p> <pre>autodeploy-register.exe -R -a vCenter-IP -p vCenter-Port -u user_name -w password -s setup-file-path</pre>
<b>VMware vCenter Server Appliance</b>	Restart the Auto Deploy daemon <code>/etc/init.d/vmware-rbd-watchdog</code> . You can start the daemon directly or use the <b>Start ESXi Services</b> and <b>Stop ESXi Services</b> vCenter Server Appliance buttons.

## Use Hosts with Static IP Addresses

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 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.
- 7 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.

## 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.

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 Services 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 73.

---

**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.

---

## 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 On the vCenter Server Appliance, unregister the built-in Auto Deploy server from a Linux command prompt.

Auto Deploy status	Action
<b>Auto Deploy has never been started on the appliance</b>	Run this command. <code>autodeploy-register --unregister -a localhost -l</code>
<b>Auto Deploy is running on the appliance</b>	Stop Auto Deploy and unregister by running these commands. <code>service vmware-rdb-watchdog stop</code> <code>chkconfig vmware-rdb-watchdog off</code> <code>autodeploy-register --unregister -a localhost -l</code>

By default, the Auto Deploy daemon is not running.

- 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

- ◆ At the Linux command prompt on the vCenter Server appliance, specify the target vCenter Server system, and provide the user name and password for the vCenter Server system.

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

## Customizing Hosts with Answer Files

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. 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.

### Setting Host Profiles to Prompt for User Input

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 5-3.** 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 <b>Storage configuration</b> and click <b>iSCSI Initiator Configuration</b>
<b>IQN name</b>	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.	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 <b>Add Profile</b> .  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.
<b>CHAP information</b>	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.	3 Set up the initiator. For many fields, the user is prompted when you apply the profile.

---

**Table 5-4.** 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.	<ol style="list-style-type: none"> <li>1 Create a subprofile. <ol style="list-style-type: none"> <li>a Click <b>Storage configuration</b>.</li> <li>b Click <b>Native Multipathing (NMP)</b>.</li> <li>c Click <b>Path Selection Policy (PSP) configuration</b>.</li> <li>d Right-click <b>Fixed PSP Configuration</b> and select <b>Add Profile</b>.</li> </ol> </li> <li>2 In the profile's Preferred Path window, select <b>Prompt the user for adapter and target IDs on the host</b>.</li> </ol>
Configure FCoE adapter activation based on a user-specified MAC address.	<ol style="list-style-type: none"> <li>1 Open <b>Storage configuration</b>.</li> <li>2 Open <b>Software FCoE configuration</b>.</li> <li>3 Open <b>Adapter Configuration</b>.</li> <li>4 If no activation profile exists, right-click <b>Activation Profile</b> and select <b>New Profile</b>.</li> <li>5 Open the profile and click <b>Policy Profile</b>.</li> <li>6 Select <b>Activation policy based on adapter MAC address</b> from the drop-down menu.</li> </ol>

**Table 5-5.** 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.	<ol style="list-style-type: none"> <li>1 Open <b>Security configuration</b>.</li> <li>2 Click <b>Administrator password</b>.</li> <li>3 Select <b>User Input Password to be Used to Configure Administrator Password</b>.</li> </ol>
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.	<ol style="list-style-type: none"> <li>1 Create a user profile by right-clicking User Configuration and selecting <b>Add Profile</b>.</li> <li>2 Configure the user by selecting one of the options. <ul style="list-style-type: none"> <li>■ <b>Assigned fixed user configurations</b> is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear.</li> <li>■ <b>Assign advanced fixed user configurations</b> is for users of ESXi 5.0 systems.</li> <li>■ <b>Specify the user configuration in the profile but prompt for password during host configuration</b> allows you to specify the information about the user but prompt for a password on each host.</li> </ul> </li> </ol>
Prompt the user for credentials when the host joins the Active Directory domain.	<ol style="list-style-type: none"> <li>1 Set the Authentication configuration profile to use a fixed domain. <ol style="list-style-type: none"> <li>a Open <b>Authentication configuration</b>.</li> <li>b Open <b>Active Directory configuration</b>.</li> <li>c Click <b>Domain Name</b>.</li> <li>d Select <b>Configure a fixed domain name</b>.</li> </ol> </li> <li>2 Set the method for joining the domain to prompt the user. <ol style="list-style-type: none"> <li>a Open <b>Authentication configuration</b>.</li> <li>b Open <b>Active Directory configuration</b>.</li> <li>c Click <b>JoinDomain Method</b>.</li> <li>d Select <b>Use user specified AD credentials to join the host to domain</b>.</li> </ol> </li> </ol>



**Table 5-6.** 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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host port group</b>.</li> <li>3 Open <b>Management Network</b>.</li> <li>4 Click <b>Determine how MAC address for vmknic should be decided</b>.</li> <li>5 Select how the system manages the MAC address. <ul style="list-style-type: none"> <li>■ <b>User specified MAC Address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for the MAC Address if no default is available</b></li> </ul> </li> </ol>
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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host port group</b>.</li> <li>3 Open <b>Management Network</b>.</li> <li>4 Open <b>IP address settings</b>.</li> <li>5 Click <b>IPv4 address</b>.</li> <li>6 Select how the system manages the IPv4 address. <ul style="list-style-type: none"> <li>■ <b>User specified IPv4 address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for the IPv4 address if no default is available</b></li> </ul> </li> </ol>
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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host port group</b>.</li> <li>3 Open <b>Management Network</b>.</li> <li>4 Open <b>IP address settings</b>.</li> <li>5 Click <b>Static IPv6 address</b>.</li> <li>6 Select how the system manages the IPv6 address. <ul style="list-style-type: none"> <li>■ <b>User specified IPv6 address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for the IPv6 address if no default is available</b></li> </ul> </li> </ol>
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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>DNS configuration</b>.</li> <li>3 In the right panel, click <b>Edit</b> next to What is the name of this host.</li> <li>4 Select how the system manages the DNS configuration. <ul style="list-style-type: none"> <li>■ <b>Prompt the user for host name if default is not available</b></li> <li>■ <b>User specified host name to be used while applying the configuration</b></li> </ul> </li> </ol>
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 <b>Add profile</b> 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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host virtual NIC</b>.</li> <li>3 Open <i>doSwitch:doPortGroup</i>  The available port group depends on your environment.</li> <li>4 Click <b>Determine how MAC address for vmknic should be decided</b>.</li> <li>5 Select how the system manages the MAC address for the distributed switch. <ul style="list-style-type: none"> <li>■ <b>User specified MAC address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for the MAC address if no default is available</b></li> </ul> </li> </ol>

**Table 5-6.** 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 <b>Add profile</b> 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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host virtual NIC</b>.</li> <li>3 Open <i>dvSwitch:dvPortGroup</i>  The available port group depends on your environment.</li> <li>4 Open <b>IP address settings</b>.</li> <li>5 Click <b>IPv4 address</b>.</li> <li>6 Select how the system handles the IPv4 address for the distributed switch. <ul style="list-style-type: none"> <li>■ <b>User specified IPv4 address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for IPv4 address if no default is available</b></li> </ul> </li> </ol>
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 <b>Add profile</b> 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.	<ol style="list-style-type: none"> <li>1 Open <b>Networking configuration</b>.</li> <li>2 Open <b>Host virtual NIC</b>.</li> <li>3 Open <i>dvSwitch:dvPortGroup</i>  The available port group depends on your environment.</li> <li>4 Open <b>IP address settings</b>.</li> <li>5 Click <b>Static IPv6 address</b>.</li> <li>6 Select how the system manages the IPv6 address for the distributed switch. <ul style="list-style-type: none"> <li>■ <b>User specified IPv6 address to be used while applying the configuration</b></li> <li>■ <b>Prompt the user for IPv6 address if no default is available</b></li> </ul> </li> </ol>

## Auto Deploy Best Practices and Security Consideration

Follow best practices when installing vSphere Auto Deploy and when using Auto Deploy with other vSphere components. Follow security guidelines 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.

- For hosts that can be part of a vSphere cluster, follow these steps.
  - a Enable vSphere HA on the cluster.
  - b Include the `vmware-fdm` VIB in the image profile that you want to use.
  - c Use PowerCLI to write a rule that assigns that image profile to the target hosts.

If the image profile does not include the `vmware-fdm` VIB, a warning message appears on the PowerCLI console when you run the `New-DeployRule` or `Copy-DeployRule` cmdlet. The message includes information on how to add the VIB. See [“vmware-fdm Warning Message When You Assign an Image Profile to Auto Deploy Host,”](#) on page 102.

- 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.
  - Deploy the vCenter Server system and the Auto Deploy server on the same system. This approach is especially well suited for a proof of concept environment.
  - 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.

<b>IP Address Allocation</b>	Using DHCP reservations is highly recommended for address allocation. Fixed IP addresses are supported by the answer file mechanism, but providing input for each host is cumbersome and not recommended.
<b>VLAN Considerations</b>	<p>Using Auto Deploy in environments that do not use VLANs is highly recommended. Do not use VLAN tagged networks at the boot NIC.</p> <p>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.</p>

## Auto Deploy and VMware Tools Best Practices

See the VMware Knowledge Base 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 proxies can be used with Auto Deploy to 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 requests through to the Auto Deploy server.

Configure the hosts to boot off the reverse proxy by modifying the TFTP tramp file. When you click **Download TFTP ZIP** in the vSphere Client, the system downloads the ZIP file that contains the tramp file. See [“Prepare Your System and Install the Auto Deploy Server,”](#) on page 73. Change the URLs in that file to refer to the address of the reverse proxy.

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

- 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.

Configuration	
BIOS DHCP File Name:	undionly.kpxe.vmw-hardwired
EFI DHCP File Name:	snponly64.efi.vmw-hardwired
gPXE Boot URL:	https://192.168.1.2:6501/vmw/rbd/tramp
Cache Size:	2.00 GiB
Cache Space In-Use:	<1 MiB
Actions	
<a href="#">Download TFTP Boot Zip</a>	
<a href="#">Download AutoDeploy Log Files</a>	

- 5 In the Auto Deploy page, click **Download AutoDeploy Log 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 88 and [“Set Up ESXi Dump Collector from the Host Profiles Interface,”](#) on page 90.

## 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 98 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 101.

## 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 answer file are included in the boot image if Auto Deploy rules are set up to provision the host with a host profile or answer file.
  - The administrator (root) password and user passwords that are included with host profile and answer files are MD5 encrypted.
  - Any other passwords associated with profiles are in the clear. If you set 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.

The files that contain the host profile and answer file information are stored on disk in an obfuscated form. The files can be retrieved only as part of the `waiter.tgz` file that is generated for each host. The raw files are not accessible through the web server. However, malicious code can pretend to be a particular host and download a host's `waiter.tgz` file. The information in the `waiter.tgz` file can then be used to compromise the ESXi host.

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 reevaluate 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 gPXE. The host is not redirected to the Auto Deploy server.

### Problem

During boot, a host that you want to provision with Auto Deploy loads gPXE. 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.

## vmware-fdm Warning Message When You Assign an Image Profile to Auto Deploy Host

When users run PowerCLI cmdlets that assign an image profile to one or more hosts, an error results if the vmware-fdm package is not part of the image profile. This package is required if you use the Auto Deploy host with vSphere HA.

### Problem

When users write or modify rules to assign an image profile to one or more Auto Deploy hosts, the following error appears:

WARNING: The supplied image profile does not contain the "vmware-fdm" software package, which is required for the vSphere HA feature. If this image profile is to be used with hosts in a vSphere HA cluster, you should add the vmware-fdm package to the image profile. The vmware-fdm package can be retrieved from the software depot published by this vCenter Server at the following URL:

`http://<VC-Address>/vSphere-HA-depot`

You can use the `Add-EsxSoftwarePackage` cmdlet to add the package to the image profile and then update any hosts or rules that were using the older version of the profile.

### Cause

The image profile does not include the `vmware-fdm` software package, which is required by vSphere HA.

### Solution

If you will not use the Auto Deploy hosts in an environment that uses vSphere HA, you can ignore the warning.

If you will use the Auto Deploy hosts in an environment that uses vSphere HA, follow the instructions in the warning.

- 1 At the PowerCLI command prompt, add the software depot that includes the `vmware-fmd` package.

```
Add-EsxSoftwareDepot http://VC-Address/vSphere-HA-depot
```

- 2 (Optional) If the image profile that generated the warning is read-only, clone the image profile.

```
New-EsxImageProfile -CloneProfile My_Profile -name "Test Profile Error Free"
```

This example clones the profile named `My_Profile` and assigns it the name `Test Profile Error Free`.

- 3 Run `Add-EsxSoftwarePackage` to add the package to the image profile.

```
Add-EsxSoftwarePackage -ImageProfile "Test Profile Error Free" -SoftwarePackage vmware-fdm
```

## 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 gPXE information, but reboots after five minutes.

### Problem

A host to be provisioned with Auto Deploy boots from gPXE and displays gPXE 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.

See *vSphere Installation and Setup* documentation for details about vSphere Auto Deploy.

## 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 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 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 you provision with Auto Deploy stops at the gPXE boot screen.

### Problem

When you attempt to boot a host provisioned with Auto Deploy, the boot process stops at the gPXE 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 inaccessible.

### 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 it if it is not running.
- 3 Open a Web browser and 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 encounter 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 are using Auto Deploy to provision the ESXi hosts in your environment, you might, in some situations, encounter a problem with the Auto Deploy database.

---

**NOTE** 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 log by using the vSphere Client. See [“Auto Deploy Best Practices,”](#) on page 98.
- 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
<b>vCenter Server appliance</b>	/var/lib/rbd
<b>Microsoft Windows</b>	The data directory you selected during installation. To find this directory, enter 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 later.
- 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.

## 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.

## 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 included in the setup.

You need the following hardware and software for your proof of concept setup.

- vCenter Server 5.0 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.



**CAUTION** If you set up Auto Deploy to boot a host, vSphere checks each of the local storage devices on the system for existing partitions. To avoid the possibility of data loss, vSphere does not create partitions under the following conditions:

- A local storage device contains a GPT partition map.
- A local storage device contains an MBR partition table that defines at least one partition.
- Storage is remote.

If hosts have local storage with a partition table that vSphere does not recognize, such as Linux Logical Volume Manager, vSphere overwrites the storage and creates new partitions. To make sure local storage is not considered for partitioning, you can physically disconnect that storage.

- 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 5.0 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.

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 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,”](#) on page 114.

### Prerequisites

Make sure your system meets the requirements in the Preinstallation Checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.

### 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 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 110.

## 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.
 

```
powershell <Enter>
Set-ExecutionPolicy RemoteSigned <Enter>
Exit <Enter>
```
- 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 76. 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 110.

## Prepare Auto Deploy Target Hosts

You must prepare all target hosts for Auto Deploy.

### Prerequisites

Hosts 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 111.

## Prepare the DHCP Server

The DHCP Server in your proof of concept environment must be set up to serve each target host with an gPXE 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.

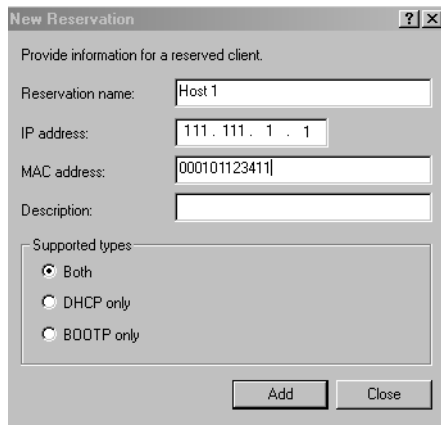
### Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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**.

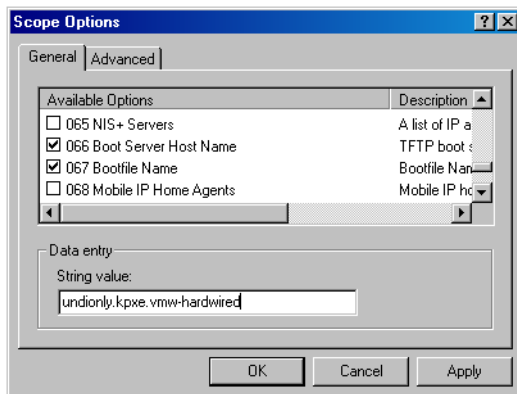
- c In the New Reservation window, specify a name, IP address, and the MAC address for one of the hosts. Do not include the colon (:) in the MAC address.



- 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 you installed in the String value field below.



- e Click **067 Bootfile Name** and enter **undionly.kpxe.vmw-hardwired**.  
The undionly.kpxe.vmw-hardwired gPXE 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 113.

**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 108 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 113.

**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.

**Prerequisites**

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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
<b>Virtual</b>	Attach the CD-ROM drive to the ISO, either by using the vSphere Client or from the datastore.
<b>Physical</b>	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

- If the vSphere Client software is not installed, install it now.
- Configure the Auto Deploy and TFTP environment. See [“Configure the Auto Deploy and TFTP Environment,”](#) on page 114.

## Configure the Auto Deploy and TFTP Environment

You must download a TFTP Boot ZIP file from your Auto Deploy server. The customized TFTP server serves the boot images Auto Deploy provides.

#### Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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.

Configuration	
BIOS DHCP File Name:	undionly.kpxe.vmw-hardwired
EFI DHCP File Name:	snponly64.efi.vmw-hardwired
gPXE Boot URL:	https://192.168.1.2:6501/vmw/rbd/tramp
Cache Size:	2.00 GiB
Cache Space In-Use:	<1 MiB
Actions	
<a href="#">Download TFTP Boot Zip</a>	
<a href="#">Download AutoDeploy Log Files</a>	

- 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 115.

## 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 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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-5.0.0-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-5.0.0-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 116.

## 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 <code>-Name</code> parameter.																		
Item	One or more items, specified with the <code>-Item</code> 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. <table> <tr> <td><b>vendor</b></td><td>Machine vendor name.</td></tr> <tr> <td><b>model</b></td><td>Machine model name.</td></tr> <tr> <td><b>serial</b></td><td>Machine serial number.</td></tr> <tr> <td><b>hostname</b></td><td>Machine hostname.</td></tr> <tr> <td><b>domain</b></td><td>Domain name.</td></tr> <tr> <td><b>ipv4</b></td><td>IPv4 address of the machine.</td></tr> <tr> <td><b>mac</b></td><td>Boot NIC MAC address.</td></tr> <tr> <td><b>asset</b></td><td>Machine asset tag.</td></tr> <tr> <td><b>oemstring</b></td><td>OEM-specific strings in the SMBIOS.</td></tr> </table> <p>Specify <code>-AllHosts</code> to apply the item or items to all hosts.</p>	<b>vendor</b>	Machine vendor name.	<b>model</b>	Machine model name.	<b>serial</b>	Machine serial number.	<b>hostname</b>	Machine hostname.	<b>domain</b>	Domain name.	<b>ipv4</b>	IPv4 address of the machine.	<b>mac</b>	Boot NIC MAC address.	<b>asset</b>	Machine asset tag.	<b>oemstring</b>	OEM-specific strings in the SMBIOS.
<b>vendor</b>	Machine vendor name.																		
<b>model</b>	Machine model name.																		
<b>serial</b>	Machine serial number.																		
<b>hostname</b>	Machine hostname.																		
<b>domain</b>	Domain name.																		
<b>ipv4</b>	IPv4 address of the machine.																		
<b>mac</b>	Boot NIC MAC address.																		
<b>asset</b>	Machine asset tag.																		
<b>oemstring</b>	OEM-specific strings in the SMBIOS.																		

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 VMware PowerCLI.

#### Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.

- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 for the complete list.
- Make sure you can access the ESXi 5.0 software you downloaded earlier 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 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-5.0.0-XXXXX-standard with the image profile you want to use.

**New-DeployRule -Name "InitialBootRule" -Item "Esxi-5.0.0-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 117.

## 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 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 for the complete list.

### Procedure

- 1 Open a console session to the physical host you want to use as the first ESXi target host, boot the host, and look for messages that indicate a successful gPXE 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 gPXE 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 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 101.

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 118.

## Configure the Proof of Concept Reference Host

You can customize the first ESXi host 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.

<b>Shared settings</b>	Specify settings all hosts share and save a host profile for the host.
<b>Host-specific settings</b>	You can 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. Those settings are saved in an answer file associated the reference host profile. See <a href="#">“Customizing Hosts with Answer Files,”</a> on page 95.

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 update the answer file to be prompted for the host-specific information.

---

**NOTE** Administrators cannot directly access or manipulate answer files. Use the vSphere Client Host Profiles UI to work with answer files.

---

### Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 for the complete list.

### Procedure

- 1 Use the vSphere 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
<b>Networking</b>	Configure the following networking components. <ul style="list-style-type: none"> <li>■ Base virtual switch and management port group for VMkernel.</li> <li>■ Storage network port group for VMkernel.</li> <li>■ Virtual machine networking port group.</li> <li>■ Any additional virtual switches and port groups.</li> <li>■ Distributed switches, if necessary (transfer port groups to distributed switches if you use them).</li> </ul>
<b>Storage</b>	Configure shared storage.
<b>Time settings</b>	Configure your time settings.
<b>Security</b>	Configure the security profile.
<b>Authentication</b>	Configure authentication.

Configuration	Description
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 [“Create a Host Profile,”](#) on page 119.

## Create a Host Profile

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 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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
<b>Creation Method</b>	Create Profile from existing host.
<b>Specify Reference Host</b>	Select the host you just configured.
<b>Profile Details</b>	Name the profile ESXiGold and add a description.
<b>Ready to Complete</b>	Review the information and click <b>Finish</b> .

- 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 120.

## Create a Rule for Other Target Hosts

You can create a rule that applies the previously verified image profile and the host profile 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 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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 at the prompt.

```
Connect-VIServer -Server your_vc_hostname -User username -Password password <Enter>
Add-EsxSoftwareDepot path:\VMware-Esxi-5.0.0-xxxxx-depot.zip <Enter>
```

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) Display the rules in the active ruleset by typing the following cmdlet at the prompt.

```
Get-DeployRuleset <Enter>
```

- 4 Create the 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.

```
New-DeployRule -name "Production01Rule" -item "image_profile", ESXiGold, target_cluster -
Pattern "ipv4=IP_range" <Enter>
```

Option	Description
<b>image_profile</b>	The ESXi image profile you used in the first deploy rule.
<b>target_cluster</b>	Name of the cluster in vCenter Server to which you want to add all hosts.
<b>IP_range</b>	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-5.0.0-XXXXXX-standard, Compute01, ESXiGold}
```

### What to do next

Provision all hosts and create an answer file for each host. See [“Provision All Hosts and Create Answer Files,”](#) on page 121.

## Provision All Hosts and Create Answer Files

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 update the answer file to be prompted for the information. The system creates the answer file and associates it with the host.

### Prerequisites

- Make sure your system meets the requirements in the preinstallation checklist. See [“Proof of Concept Preinstallation Checklist,”](#) on page 108.
- Perform all preceding proof of concept setup tasks. See [“Auto Deploy Proof of Concept Setup,”](#) on page 108 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 answer file. 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

---

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,”](#) on page 123
- [“Image Builder Installation and Usage,”](#) on page 130
- [“Image Builder Common Tasks,”](#) on page 131
- [“Image Builder Workflows,”](#) on page 138

## 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 124.

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.**

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.

**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 5.0 base VIB and the custom extensions. 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.

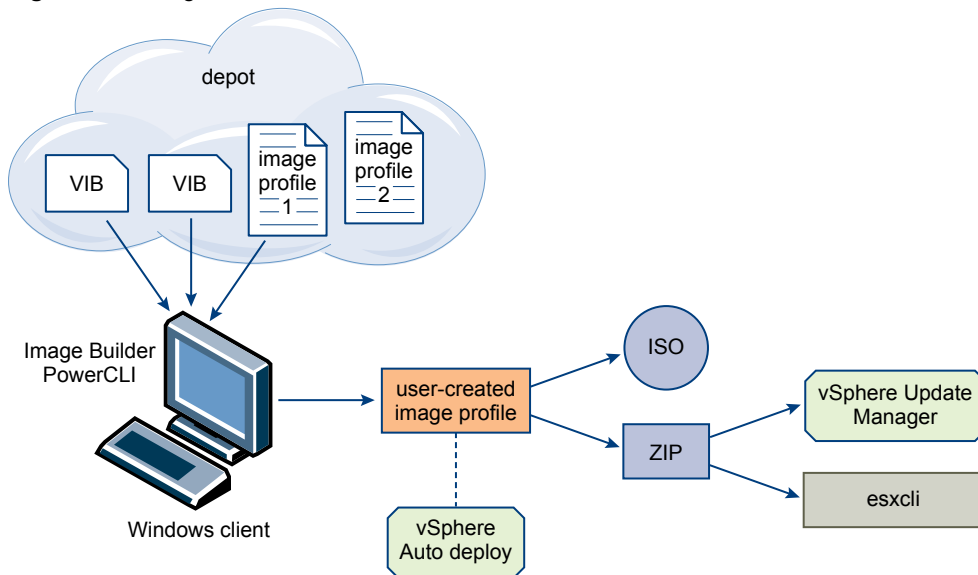
**Input.**

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 vib` 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 128.

### 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 127.

### 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
<code>Add-EsxSoftwareDepot</code>	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.
<code>Remove-EsxSoftwareDepot</code>	Disconnects from the specified software depot.
<code>Get-EsxSoftwarePackage</code>	Returns a list of software package objects (VIBs). Use this cmdlet's options to filter the results.
<code>Get-EsxImageProfile</code>	Returns an array of <code>ImageProfile</code> objects from all currently added depots.
<code>New-EsxImageProfile</code>	Creates a new image profile. In most cases, creating a new profile by cloning an existing profile is recommended. See <a href="#">“Create an Image Profile,”</a> on page 131.
<code>Set-EsxImageProfile</code>	Modifies a local <code>ImageProfile</code> object and performs validation tests on the modified profile. The cmdlet returns the modified object but does not persist it.
<code>Export-EsxImageProfile</code>	Exports an image profile as either an ESXi ISO image for ESXi installation, or as a ZIP file.
<code>Compare-EsxImageProfile</code>	Returns an <code>ImageProfileDiff</code> structure that shows whether the two profiles have the same VIB list and acceptance level. See <a href="#">“Acceptance Levels,”</a> on page 127.
<code>Add-EsxSoftwarePackage</code>	Adds one or more new packages (VIBs) to an existing image profile.
<code>Remove-EsxSoftwarePackage</code>	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 5.0 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 127

#### 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.

<b>VMwareCertified</b>	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.
<b>VMwareAccepted</b>	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.
<b>PartnerSupported</b>	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.
<b>CommunitySupported</b>	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 <a href="#">“Acceptance Levels,”</a> on page 127.
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 <code>Set-ESXImageProfile -ReadOnly</code> 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: <code>package-name[&lt;&lt; &lt;= &gt;= &gt;&gt;version]</code>
Depends	SoftwareConstraint[]	List of VIBs that must be installed at the same time as this VIB. Same constraint format as <code>Conflicts</code> 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.
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.
Summary	System.String	One-line summary of the VIB.
Tag	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.

## 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 <code>Compare-EsxImageProfile</code> .
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 <code>Compare-EsxImageProfile</code> .
OnlyInRef	System.String[]	List of VIBs found only in the first profile that you passed to <code>Compare-EsxImageProfile</code> .
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 <code>Compare-EsxImageProfile</code> .
UpgradeFromRef	System.String[]	List of VIBs in the second profile that are upgrades from VIBs in the first profile.

## 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 you 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 1.0 or 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 130. 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 138 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 130.
- 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 130.

## 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 <b>Add-EsxSoftwareDepot -DepotUrl <i>depot_url</i></b> .
ZIP file	a Download the ZIP file to a local file path. b Run <b>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</b>

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 138 for some examples of filtering.

Customize the image profile by adding or removing VIBs. See [“Add VIBs to an Image Profile,”](#) on page 132.

## 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

## Procedure

- 1 Run `Add-EsxSoftwareDepot` for each depot you want to work with.

Depot Type	Cmdlet
Remote depot	Run <code>Add-EsxSoftwareDepot -DepotUrl <i>depot_url</i></code> .
ZIP file	<ol style="list-style-type: none"> <li>a Download the ZIP file to a local file path.</li> <li>b Run <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code></li> </ol>

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 and make changes to the clone if the image profile is read only.

**`New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"`**

Image profiles published by VMware and its partners are read only.

- 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

## Procedure

- 1 Run `Add-EsxSoftwareDepot` to connect to the depot that contains the image profile to export.

Depot Type	Cmdlet
Remote depot	Run <code>Add-EsxSoftwareDepot -DepotUrl <i>depot_url</i></code> .
ZIP file	<ol style="list-style-type: none"> <li>a Download the ZIP file to a local file path.</li> <li>b Run <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code></li> </ol>

The cmdlet returns one or more `SoftwareDepot` objects.

- 2 Run `Export-EsxImageProfile` to export the image profile.

To build...	Run...
ISO images	<code>Export-EsxImageProfile</code> with the <code>-ExportToIso</code> parameter.
Offline depot ZIP files	<code>Export-EsxImageProfile</code> with the <code>-ExportToBundle</code> 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

### 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 137.

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 136. 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.	<code>esxcli --server=<i>server_name</i> software sources vib list --depot=<i>depot_URL</i></code>
List information for a specified VIB.	<code>esxcli --server=<i>server_name</i> software sources vib list --viburl=<i>vib_URL</i></code>
List information for all image profiles.	<code>esxcli --server=<i>server_name</i> software sources profile list --depot=<i>depot_URL</i></code>
List information for a specified image profile.	<code>esxcli --server=<i>server_name</i> software sources profile get --depot=<i>depot_URL</i> --profile=<i>profile_name</i></code>

- 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

## Procedure

- 1 Run `Add-EsxSoftwareDepot` for each depot you want to work with.

Depot Type	Cmdlet
Remote depot	Run <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
ZIP file	<ol style="list-style-type: none"> <li>a Download the ZIP file to a local file path.</li> <li>b Run <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.</li> </ol>

- 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 127.

## 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

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 127.
- 6 Retrieve software packages released before or after a certain date by using the `ReleasedBefore` or `ReleasedAfter` parameter.  
**Get-EsxSoftwarePackage -ReleasedAfter 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 -ReleasedAfter 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 130.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See [“Using Image Builder Cmdlets,”](#) on page 130.

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**

Name		Vendor	Last Modified	Acceptance
Level				
ESX-meta-5.0.zip Profile #1	vendor1	6/13/2010 12:...	PartnerSupported	
ESX-meta-5.0.zip Profile #2	vendor2	6/13/2010 12:...	PartnerSupported	
base-tbd-v1	vendor1	6/13/2010 12:...	CommunitySupported	
ESX-meta-5.1.zip Profile #1	vendor1	6/13/2010 12:...	PartnerSupported	
....				

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 and a name for the new profile.

**\$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42"**

- 6 Display the newly created image profile.

**Get-EsxImageProfile**

Name	Vendor	Last Modified	Acceptance Level
-----	-----	-----	-----
Test Profile 42	user1	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"
$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 130.
- 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 131 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 -ReleasedAfter 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 -ReleasedAfter 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 130.
- 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 141 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

---

These topics provide information about using the direct console user interface and configuring defaults for ESXi.

This chapter includes the following topics:

- [“ESXi Autoconfiguration,”](#) on page 145
- [“About the Direct Console ESXi Interface,”](#) on page 146
- [“Set the Password for the Administrator Account,”](#) on page 148
- [“Configuring the BIOS Boot Settings,”](#) on page 149
- [“Host Fails to Boot After You Install ESXi in UEFI Mode,”](#) on page 150
- [“Network Access to Your ESXi Host,”](#) on page 150
- [“Configure the Network Settings on a Host That Is Not Attached to the Network,”](#) on page 151
- [“Managing ESXi Remotely,”](#) on page 151
- [“Configuring Network Settings,”](#) on page 152
- [“Storage Behavior,”](#) on page 156
- [“View System Logs,”](#) on page 159
- [“Configure Syslog on ESXi Hosts,”](#) on page 159
- [“Enable Lockdown Mode Using the Direct Console,”](#) on page 160
- [“Enable ESXi Shell and SSH Access with the Direct Console User Interface,”](#) on page 161
- [“Set the Host Image Profile Acceptance Level,”](#) on page 161
- [“Reset the System Configuration,”](#) on page 162
- [“Remove All Custom Packages on ESXi,”](#) on page 163
- [“Disable Support for Non-ASCII Characters in Virtual Machine File and Directory Names,”](#) on page 163
- [“Disable ESXi,”](#) on page 163

## 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 147  
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 Using the vSphere Client](#) on page 147  
When you use the vSphere Client to redirect the direct console to a serial port, the boot option you set persists after subsequent reboots.
- [Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy](#) on page 148  
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 Using the vSphere Client,”](#) on page 147

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

When you use the vSphere Client to redirect the direct console to a serial port, the boot option you set persists after subsequent reboots.

You can redirect the direct console to either of the serial ports com1 or com2.

The serial port must not be in use for serial logging and debugging, or for ESX Shell (tty1Port).

#### Prerequisites

Verify that you can access the host from the vSphere Client. The serial port must 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 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
<b>If you are using the installable version of ESXi</b>	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.
<b>If you are using ESXi Embedded</b>	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: <ul style="list-style-type: none"> <li>■ You do not have a DHCP server.</li> <li>■ The ESXi host is not connected to a DHCP server.</li> <li>■ Your connected DHCP server is not functioning properly.</li> </ul>	<p>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.</p> <p>You can override the link local IP address by configuring a static IP address using the direct console.</p>

**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.	<p>During the autoconfiguration phase, the software assigns a DHCP-configured IP address.</p> <p>You can make the initial connection by using the DHCP-configured IP address. Then you can configure a static IP address.</p> <p>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.</p>
Your security deployment policies do not permit unconfigured hosts to be powered on the network.	Follow the setup procedure in <a href="#">“Configure the Network Settings on a Host That Is Not Attached to the Network,”</a> on page 151.

## 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 to 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 206
- [“Install vCenter Server,”](#) on page 206
- [“Download the vSphere Client,”](#) on page 212
- [“Install the vSphere Client,”](#) on page 212
- [“Install and Start the vSphere Web Client,”](#) on page 213

## 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 `vmnicN`, 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 26

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**.

## 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`, `sfcdbd`, `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 5.0 differs significantly from partitioning for new installations of ESXi 5.0. 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	<p>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 <a href="#">“About the Scratch Partition,”</a> on page 157. The VFAT scratch partition is created only on the disk from which the ESXi host is booting.</p> <p><b>NOTE</b> To create the VMFS volume and scratch partition, the ESXi installer requires a minimum of 5.2GB of free space on the installation disk.</p> <p>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.</p>
ESXi Embedded	<p>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.</p>
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 5.0 differs significantly from partitioning for new installations of ESXi 5.0. 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 159.

## Configure Syslog on ESXi Hosts

All ESXi hosts run a syslog service (`vm syslogd`), 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
<b>Syslog.global.defaultRotate</b>	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
<b>Syslog.global.defaultSize</b>	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
<b>Syslog.global.LogDir</b>	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the <code>/scratch</code> directory on the local file system is persistent across reboots. The directory should be specified as <code>[datastorename] path_to_file</code> where the path is relative to the root of the volume backing the datastore. For example, the path <code>[storage1] var/log/messages</code> maps to the path <code>/vmfs/volumes/storage1/var/log/messages</code> . If no path is specified, all log files are sent to <code>/var/log</code> .
<b>Syslog.global.logDirUnique</b>	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by <b>Syslog.global.LogDir</b> . A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
<b>Syslog.global.LogHost</b>	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, <code>ssl://hostName1:514</code> . 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.
- Click **loggers**.
  - 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 `vpuser` 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** The root user is still authorized to log in to the direct console user interface when lockdown mode is enabled.

---

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 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.
- 4 Press Enter.
- 5 (Optional) Set the timeout for the ESXi Shell.

By default, the timeout for the ESXi Shell is 0 (disabled).

The timeout setting is the number of minutes that can elapse before you must log in after ESXi Shell is enabled. After the timeout period, if you have not logged in, the ESXi Shell is disabled.

---

**NOTE** If you are logged in when the timeout period elapses, your session persists. However, the ESXi Shell is disabled, preventing other users from logging in.

---

- a From the **Troubleshooting Mode Options** menu, select **Modify ESXi Shell timeout** and press Enter.
- b Type the timeout in minutes.
- c Press Enter.

## 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 127.

### 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.



## 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,”](#) on page 165
- [“Licensing ESXi Hosts,”](#) on page 165

### 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 212
  - [“Install the vSphere Client,”](#) on page 212
  - [“Start the vSphere Client,”](#) on page 213
- vSphere Web Client
  - [“Install and Start the vSphere Web Client,”](#) on page 213

### 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 77.

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 15

## About ESXi Evaluation and Licensed Modes

After you purchase a host license, VMware provides a serial number that you can use to license vSphere. You can use evaluation mode to access the full ESXi feature set, including features you have not purchased a license for.

For example, in evaluation mode, you can use vMotion, HA, DRS, and other features, even if you have not licensed those features.

The installable version of ESXi is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal USB device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host, even if you start in licensed mode rather than evaluation mode. Any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. To take full advantage of the 60-day evaluation period, you should convert to evaluation mode as soon as possible after you first power on the host. See [“Convert an ESXi Host to Evaluation Mode,”](#) on page 166.

For information about licensing the host, see the *vCenter Server and Host Management*.

## Convert an ESXi Host to Evaluation Mode

You can switch a licensed ESXi host to evaluation mode to explore all the features of ESXi, including features that you have not licensed.

See [“About ESXi Evaluation and Licensed Modes,”](#) on page 15.

### Prerequisites

The 60-day evaluation period has not expired.

### Procedure

- 1 From the vSphere Client, select the host in the inventory.
- 2 Click the **Configuration** tab.
- 3 Under Software, click **Licensed Features**.
- 4 Click **Edit** next to ESXi License Type.
- 5 Click **(No License Key)**.
- 6 Click **OK** to save your changes.

You can now access all the features of ESXi.

## 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.





## Preparing vCenter Server Databases

---

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](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 Patch and Configuration Requirements,”](#) on page 169
- [“Create a 64-Bit DSN,”](#) on page 170
- [“Configure vCenter Server to Communicate with the Local Database,”](#) on page 171
- [“About the Bundled Microsoft SQL Server 2008 R2 Express Database Package,”](#) on page 171
- [“Maintaining a vCenter Server Database,”](#) on page 171
- [“Configure DB2 Databases,”](#) on page 172
- [“Configure Microsoft SQL Server Databases,”](#) on page 180
- [“Configure Oracle Databases,”](#) on page 190

### vCenter Server Database Patch and Configuration Requirements

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

vCenter Server databases require a UTF code set.

Contact your DBA for the appropriate database credentials.

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

**Table 9-1.** Configuration Notes for Databases Supported with vCenter Server

Database Type	Configuration Notes
IBM DB2	<p>If the database is not local to the vCenter Server system, install the IBM Data Server Runtime Client.</p> <p>Install the IBM DB2 native client according to the IBM instructions for your DB2 version.</p> <p>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.</p> <p>You might need to restart the Microsoft Windows machine for the service to recognize the change in the environment variable.</p> <p>Ensure that the machine has a valid ODBC data source name (DSN) entry.</p> <p><b>NOTE</b> This database is not supported for the vCenter Server Appliance.</p>
Microsoft SQL Server 2008 R2 Express	<p>Bundled database that you can use for small deployments of up to 5 hosts and 50 virtual machines.</p> <p><b>NOTE</b> This database is not supported for the vCenter Server Appliance.</p>
Microsoft SQL Server 2005	<p>Ensure that the machine has a valid ODBC DSN entry.</p> <p>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 <a href="http://support.microsoft.com/kb/968749">http://support.microsoft.com/kb/968749</a>.</p> <p><b>NOTE</b> This database is not supported for the vCenter Server Appliance.</p>
Microsoft SQL Server 2008	<p>Ensure that the machine has a valid ODBC DSN entry.</p> <p><b>NOTE</b> This database is not supported for the vCenter Server Appliance.</p>
Oracle	<p>For Oracle 10g R2, if necessary, first apply patch 10.2.0.4 (or later) to the client and server. You can then apply patch 5699495 to the client.</p> <p>Ensure that the machine has a valid ODBC DSN entry.</p> <p>After you complete the vCenter Server installation, take the following steps:</p> <ul style="list-style-type: none"> <li>■ Apply the latest patch to the Oracle client and server.</li> <li>■ Copy the Oracle JDBC driver (ojdbc14.jar or ojdbc5.jar) to the vCenter Server installation directory, in the tomcat\lib subdirectory: <i>vCenter install location\Infrastructure\tomcat\lib</i>.</li> </ul> <p>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.</p>

## 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 172  
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 173  
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 174  
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 175  
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 176  
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 178  
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 178  
You have several steps you need to complete before you configure a connection to a remote DB2 database on Linux, UNIX, or Microsoft Windows.
- 8 [Configure a Connection to a Remote DB2 Database on Linux, UNIX, or Microsoft Windows](#) on page 179  
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 180  
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 vcdbschema.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 178 or [“Configure a Connection to a Remote DB2 Database on Linux, UNIX, or Microsoft Windows,”](#) on page 179, 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_stat1_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
process temptable0_proc_db2.sql
process temptable1_proc_db2.sql
process temptable2_proc_db2.sql
job_schedule1_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 222.)

## 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 200.

---

### 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

You have several steps you need to complete before you configure a connection to a remote DB2 database on Linux, UNIX, or Microsoft Windows.

### Prerequisites

If you are using DB2 9.5, fix pack 5 or Hotfix 22318 is required. Fix pack 7 is recommended. If you are using DB2 9.7, fix pack 2 is required. Fix pack 3a is recommended.

### 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 178.

### 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 172.

### 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 181  
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 182  
By using this recommended method, available with vCenter Server 5.0, 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 183  
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 183  
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 184  
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 185  
You can create database objects manually with this method of configuring the SQL database.

- 7 [Configure a SQL Server ODBC Connection](#) on page 188  
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 189  
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 190  
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=[vpuser], @passwd=N'vpuser!0', @defdb='VCDB',
@deflanguage='us_english'
go
ALTER LOGIN [vpuser] WITH CHECK_POLICY = OFF
go
CREATE USER [vpuser] for LOGIN [vpuser]
go
use MSDB
go
CREATE USER [vpuser] for LOGIN [vpuser]
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 182.

## Set Database Permissions By Manually Creating Database Roles and the VMW Schema

By using this recommended method, available with vCenter Server 5.0, 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 `dbo` 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 183.

### Prerequisites

Create the vCenter Server database. See [“Create a SQL Server Database and User for vCenter Server,”](#) on page 181

### 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 184

## 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 182 and [“Use a Script to Create a Microsoft SQL Server Database Schema and Roles,”](#) on page 184. 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 181

### 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 182 [“Use a Script to Create a Microsoft SQL Server Database Schema and Roles,”](#) on page 184. 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 181

### 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 188

## 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 182 and [“Use a Script to Create a Microsoft SQL Server Database Schema and Roles,”](#) on page 184.

### 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 181

### 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 188.

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 183 and [“Use a Script to Create a vCenter Server User by Using the dbo Schema and db\\_owner Database Role,”](#) on page 183.

- 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 182.

### 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 181

### 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_stat1_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
process temptable0_proc_mssql.sql
process temptable1_proc_mssql.sql
process temptable2_proc_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_schedule1_mssql.sql
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 store procedures you created in [Step 4](#), grant the execute privilege to the vCenter Server database.

```
grant execute on purge_stat1_proc to vCenter_db_user
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 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 222.

- 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 Patch and Configuration Requirements,”](#) on page 169.
- 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 181
- 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 182 and [“Use a Script to Create a Microsoft SQL Server Database Schema and Roles,”](#) on page 184
  - Option 2 (alternative): Follow the procedures in [“Set Database Permissions by Using the dbo Schema and the db\\_owner Database Role,”](#) on page 183 and [“Use a Script to Create a vCenter Server User by Using the dbo Schema and db\\_owner Database Role,”](#) on page 183.

### 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	<b>Yes</b>
Listen All	<b>Yes</b>
Keep Alive	<b>30000</b>

- 6 On the **IP Addresses** tab, make the following selections.

Active	<b>Yes</b>
TCP Dynamic Ports	<b>0</b>

- 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 191  
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 192  
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 192  
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 194  
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 194  
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 195  
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 196
- 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 194 or [“Configure an Oracle Database Connection for Remote Access,”](#) on page 194, 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_stat1_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/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_schedule1_oracle.sql
@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 222.

- 9 When prompted, provide the database user login.

The Oracle dadatabase 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 Patch and Configuration Requirements,”](#) on page 169. 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 Patch and Configuration Requirements,”](#) on page 169. 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

---

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:

- [“vCenter Server Prerequisites,”](#) on page 197
- [“Using a User Account for Running vCenter Server,”](#) on page 199
- [“Installing vCenter Server on IPv6 Machines,”](#) on page 200
- [“JDBC URL Formats for the vCenter Server Database,”](#) on page 200
- [“Configure the URLs on a Standalone vCenter Server System,”](#) on page 201
- [“Running the vCenter Server and vSphere Client Installers from a Network Drive,”](#) on page 202
- [“Required Information for Installing vCenter Server,”](#) on page 202
- [“Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail,”](#) on page 204

### vCenter Server Prerequisites

Before installing vCenter Server, review the prerequisites.

- Verify that you have the installation DVD or download the vCenter Server installer. See [“Download the vCenter Server Installer,”](#) on page 206.
- Verify that your system meets the requirements listed in [“vCenter Server and vSphere Client Hardware Requirements,”](#) on page 33 and [“vCenter Server Software Requirements,”](#) on page 36, and that the required ports are open, as discussed in [“Required Ports for vCenter Server,”](#) on page 38.
- Verify that your database meets the database requirements. See [“vCenter Server Database Patch and Configuration Requirements,”](#) on page 169 and [Chapter 9, “Preparing vCenter Server Databases,”](#) on page 169.
- Gather the information that the vCenter Server installation wizard requires. See [“Required Information for Installing vCenter Server,”](#) on page 202.
- Verify that the fully qualified domain name (FQDN) of the system where you will install vCenter Server is resolvable. To check that the FQDN is resolvable, type `nslookup your_vCenter_Server_fqdn` at a command line prompt. If the FQDN is resolvable, the `nslookup` command returns the IP and name of the domain controller machine.

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

---

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

---

- Verify that no Network Address Translation (NAT) exists between the vCenter Server system and the hosts it will manage.
- Create a vCenter Server database, unless you plan to install the bundled SQL Server 2008 R2 Express.
- If the system that you use for your vCenter Server installation belongs to a workgroup rather than a domain, not all functionality is available to vCenter Server. If assigned to a workgroup, the vCenter Server system is not able to discover all domains and systems available on the network when using some features. To determine whether the system belongs to a workgroup or a domain, right-click **My Computer**. Click **Properties** and click the **Computer Name** tab. The **Computer Name** tab displays either a Workgroup label or a Domain label.
- During the installation, verify that the connection between the machine and the domain controller is working.
- Verify that the computer name is no more than 15 characters.
- The NETWORK SERVICE account is required on the folder in which vCenter Server is installed and on the HKLM registry.
- Verify that the DNS name of the machine matches the actual computer name.
- Make sure the system on which you are installing vCenter Server is not an Active Directory domain controller.
- On each system that is running vCenter Server, make sure that the domain user account has the following permissions:
  - **Member of the Administrators group**
  - **Act as part of the operating system**
  - **Log on as a service**
- Consider whether the vCenter Server instance will be standalone or in a Linked Mode group. See [“Creating vCenter Server Linked Mode Groups,”](#) on page 220.
- 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.

## 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 199.

---

## 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

If you install vCenter Server on a system that is configured to use IPv6, vCenter Server uses IPv6. When you connect to that vCenter Server system or install more modules, you must specify the server address in IPv6 format, unless you use the fully qualified domain name.

As specified in the Remote Procedure Call (RPC) standards for IPv6 addresses, you must enclose the IPv6 address in square brackets: *[IPv6-address]*.

## 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 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](http://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/BEIJFHBB](http://download.oracle.com/docs/cd/B28359_01/java.111/b31224/urls.htm/BEIJFHBB)

## 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](http://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 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.

**Table 10-1.** Information Required for vCenter Server Installation

Data	Default	Comments
Setup Language	English	This selection controls the language only for the installer.
User name and organization	Your organization's name	Follow your organization's policy.
vCenter Server license key	None	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.
vCenter Server install location	C:\Program Files\VMware\Infrastructure	The default location varies depending on your system drive. You can change the default location during the installation. The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).
Standalone or join group	Standalone	Join a Linked Mode group to enable the vSphere Client to view, search, and manage data across multiple vCenter Server systems.
Fully qualified domain name of Directory Services for the vCenter Server group	None	Required if this instance of vCenter Server is joining a group. This is the name of a remote instance of vCenter Server. The local and remote instances will be members of a Linked Mode group.

**Table 10-1.** Information Required for vCenter Server Installation (Continued)

Data	Default	Comments
LDAP port for the Directory Services for the remote vCenter Server instance	389	Required if this instance of vCenter Server is joining a Linked Mode group. This is the remote instance's LDAP port. See <a href="#">“Required Ports for vCenter Server,”</a> on page 38.
Data source name (DSN)	None	Required to use an existing database. Not required if you are using the bundled database. Leading and trailing spaces are not supported. Remove any spaces from the beginning or end of the DSN.
Database user name	None	Required to use an existing database. Not required if you are using the bundled database. Non-ASCII characters are not supported.
Database password	None	
JDBC URL for database	None	Required to 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 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 <a href="#">“JDBC URL Formats for the vCenter Server Database,”</a> on page 200.
vCenter Server Service account information Can be the Microsoft Windows system account or a user-specified account	Microsoft Windows system account	Use a user-specified account if you plan to use Microsoft Windows authentication for SQL Server. See <a href="#">“Using a User Account for Running vCenter Server,”</a> on page 199.
Fully qualified domain name (FQDN) for the vCenter Server machine		The Fully Qualified Domain Name field displays the FQDN of the system that you are installing vCenter Server on. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message is displayed. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.
vCenter Inventory Service install location	C:\Program Files\VMware\Infrastructure	You can change the default location during the installation.
HTTPS port	443	See <a href="#">“Required Ports for vCenter Server,”</a> on page 38.
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	
vCenter Inventory Service HTTPS port	10443	

**Table 10-1.** Information Required for vCenter Server Installation (Continued)

Data	Default	Comments
vCenter Inventory Service management port	10109	
vCenter Inventory Service linked mode communication port	10111	

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

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

### Problem

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

### Cause

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

### Solution

- ◆ Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version. See [“vCenter Server Database Patch and Configuration Requirements,”](#) on page 169

# Installing vCenter Server

---

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,”](#) on page 205
- [“Download the vCenter Server Installer,”](#) on page 206
- [“Install vCenter Server,”](#) on page 206
- [“Install vCenter Server in a Virtual Machine,”](#) on page 208
- [“Download and Deploy the VMware vCenter Server Appliance,”](#) on page 209

## vCenter Server Components and Support Tools

When you install vCenter Server, other components are also installed.

The following components are installed when you install vCenter Server:

<b>VMware vCenter Server</b>	Windows service to manage ESXi and legacy ESX hosts.
<b>Microsoft .NET 3.5 SP1 Framework</b>	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.
<b>Microsoft Windows Installer version 4.5</b>	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.
<b>VMware vCenter Orchestrator</b>	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 <i>Administering vCenter Orchestrator</i> .
<b>Microsoft SQL Server 2008 R2 Express (optional)</b>	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.

The vCenter Server `autorun.exe` application includes links to install the following optional components:

<b>vSphere Client</b>	Client application used to connect to an ESXi or legacy ESX host directly, or indirectly through a vCenter Server.
<b>vSphere Web Client</b>	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.
<b>vSphere Update Manager</b>	vCenter Server component that provides security monitoring and patching support for hosts and virtual machines.
<b>vSphere ESXi Dump Collector</b>	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.
<b>vSphere Syslog Collector</b>	vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.
<b>vSphere Auto Deploy</b>	vCenter Server support tool that provisions and customizes physical hosts by loading the ESXi image directly into memory. Using Auto Deploy you can provision and reprovision hundreds of ESXi hosts very efficiently with vCenter Server.
<b>vSphere Authentication Proxy</b>	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 Server

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

### Prerequisites

See “[vCenter Server Prerequisites](#),” on page 197. Gather the information that is required to complete the installation wizard. See “[Required Information for Installing vCenter Server](#),” on page 202.

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

### Procedure

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

- 2 Select **vCenter Server™**.
- 3 Follow the prompts in the installation wizard to choose the installer language, agree to the end user patent and license agreements, enter your user name, organization name, and license key.

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

- 4 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 dialog box might appear warning you 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 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 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 is displayed when you click **Next**. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.

- 6 Either accept the default destination folders 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 (%).

---

**NOTE** 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. If you do not have enough space, your vCenter Server installation might fail.

---

- 7 Select **Create a standalone VMware vCenter Server instance** or **Join Group**.

Join a Linked Mode group to enable the vSphere Client to view, search, and manage data across multiple vCenter Server systems. See [“Creating vCenter Server Linked Mode Groups,”](#) on page 220.

---

**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.

In some cases, you can enter the IP address instead of the fully qualified domain name. To ensure connectivity, use the fully qualified domain name. For IPv6, unless both the local and the remote machine are in IPv6 mode, enter the fully qualified domain name of the remote machine instead of the IPv6 address. If the local machine has an IPv4 address and the remote machine has an IPv6 address, the local machine must support IPv4 and IPv6 mixed mode. The domain name server must be able to resolve both IPv4 and IPv6 addresses if your environment has both addressing types in a single Linked Mode group.

- 9 Enter the port numbers that you want to use or accept the default port numbers.

See [“Required Ports for vCenter Server,”](#) on page 38.

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

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

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

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

- 12 Click **Install**.

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

- 13 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, 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 211.

## 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 “[vCenter Server Prerequisites](#),” on page 197.

### 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](#),” on page 206.

## 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**.

Microsoft SQL Server and IBM DB2 are not supported for the vCenter Server Appliance.

---

**NOTE** Version 5.0.1 of the vCenter Server Appliance uses PostgreSQL for the embedded database instead of IBM DB2, which was used in vCenter Server Appliance 5.0.

---

The vCenter Server Appliance does not support Linked Mode configuration. The vCenter Server Appliance does not support IPv6.

---

**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.

---

For information about configuring the vCenter Server Appliance, see the *vCenter Server and Host Management* documentation.

### Prerequisites

- Verify that vSphere Client is installed.
- You can deploy the vCenter Server Appliance only on hosts that are running ESX version 4.x or ESXi version 4.x or later.
- 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.

### Procedure

- 1 From the vSphere 5 download page on the VMware Web site, download the .VMDK and .OVF files for the vCenter Server appliance onto your system.  
Save the .VMDK and .OVF files in the same folder.
- 2 In the vSphere Client, select **File > Deploy OVF Template** and enter the path to the .OVF file on your system.

- 3 Follow the prompts in the Deploy OVF Template wizard to create the vCenter Server Appliance.

If you do not want to commit to using the maximum 80GB of disk space at deployment, deploy the OVF with thin provisioning. In the Disk Format panel of the wizard, select **Thin provisioned format**.

## 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 make sure that you can access the vCenter Server instance.
- Check the license server configuration. A license server is required if this vCenter Server is managing ESX 3.5/ESXi 3.5 hosts. See [“Using a License Server to Manage Version 3.5 ESX or ESXi Hosts,”](#) on page 226.
- 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 226.

### 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 the `ojdbc14.jar` file is not 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. At the time of this topic's publication, the file was available at [http://www.oracle.com/technology/software/tech/java/sqlj\\_jdbc/htdocs/jdbc101040.html](http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc101040.html).

### 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,”](#) on page 212
- [“Creating vCenter Server Linked Mode Groups,”](#) on page 220
- [“Using a License Server to Manage Version 3.5 ESX or ESXi Hosts,”](#) on page 226

- [“VMware vCenter Management Webservices Service Fails to Start,”](#) on page 226
- [“Back Up the Inventory Service Database on Windows,”](#) on page 227
- [“Restore an Inventory Service Database Backup on Windows,”](#) on page 227
- [“Back Up the Inventory Service Database on Linux,”](#) on page 228
- [“Restore an Inventory Service Database Backup on Linux,”](#) on page 228
- [“Update the vCenter Inventory Service URL Configuration,”](#) on page 229
- [“Reset the vCenter Inventory Service Database,”](#) on page 229

## 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
<b>If you are installing from the vCenter Server installer</b>	<ol style="list-style-type: none"> <li>a In the software installer directory, double-click the <code>autorun.exe</code> file.</li> <li>b Select <b>vSphere™ Client</b>.</li> <li>c Click <b>Install</b>.</li> </ol>
<b>If you downloaded the vSphere Client</b>	Double-click the <code>VMware-viclient-build number.exe</code> 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
<b>Log in to an ESXi host.</b>	Log in as root or as a normal user.
<b>Log in to a vCenter Server system as the administrator.</b>	<ol style="list-style-type: none"> <li>a Type the vCenter Server IP address or host name.</li> <li>b Type your user name and password.</li> </ol>

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 and Start the vSphere Web Client

The vSphere Web Client enables you to connect to a vCenter Server system to manage an ESXi host through a browser.

### Prerequisites

- Download the vCenter Server installer.
- Verify that you are a member of the Administrators group on the system.

- 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 37. The vSphere Web Client requires a 64-bit operating system for installation.

### Procedure

- 1 In the software installer directory, double-click the `autorun.exe` file to start the installer.
- 2 Select **VMware vSphere® Web Client (Server)** and click **Install**.
- 3 Follow the wizard prompts to complete the installation.  
When the vSphere Web Client installation is finished, a browser opens.
- 4 Register one or more vCenter Servers on the vSphere Web Client Administration Application page in the browser.

---

**NOTE** If the vCenter Server uses IPv6, you must specify the server address in IPv6 format, unless you use the fully qualified domain name. As specified in the Remote Procedure Call (RPC) standards for IPv6 addresses, you must enclose the IPv6 address in square brackets: `[IPv6-address]`.

---

- 5 If the browser fails to open or to display the Administration Application page correctly, open the application from the shortcut:

From the Windows **Start** menu, select **Programs > VMware > VMware vSphere Web Client > vSphere Administration Application**.

## 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*.

### 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**.
- 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 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.

---

**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 88. 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 5.0.

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 36 and [“vCenter Server and vSphere Client Hardware Requirements,”](#) 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:

- 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 ESXi™ Dump Collector** and click **Install**.
- 3 Follow the wizard prompts to complete the installation.

## Install 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.

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 36 and [“vCenter Server and vSphere Client Hardware Requirements,”](#) 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:

- 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® Syslog Collector** and click **Install**.

- 3 Follow the wizard prompts to complete the installation.

## Install 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.

You must install the Auto Deploy feature separately for each instance of vCenter Server that you plan to use the feature with. Auto Deploy is not supported with vCenter Server versions earlier than version 5.0. Auto Deploy supports both IPv4 and IPv6.

### 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 36 and [“vCenter Server and vSphere Client Hardware Requirements,”](#) on page 33.

Gather the following information to complete the installation:

- 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® Auto Deploy** and click **Install**.
- 3 Follow the wizard prompts to complete the installation.

## Install 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.

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 vSphere Auto Deploy,”](#) on page 218.
- 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 36 and [“vCenter Server and vSphere Client Hardware Requirements,”](#) 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:

- 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.

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**.

## 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** Linked Mode groups that contain both vCenter Server 5.0 and earlier versions of vCenter Server are not supported. The vSphere Client does not function correctly with vCenter Servers in groups that have both version 5.0 and earlier versions of vCenter Server. Do not join a version 5.0 vCenter Server to earlier versions of vCenter Server, or an earlier version of vCenter Server to a version 5.0 vCenter Server. Upgrade any vCenter Server instance to version 5.0 before joining it to a version 5.0 vCenter Server.

## Linked Mode Considerations for vCenter Server

Consider several issues before you configure a Linked Mode group.

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

- If you upgrade a vCenter Server that is part of a Linked Mode group, it will be removed from the group. vCenter Server does not support Linked Mode groups that contain both version 5.0 and earlier versions of vCenter Servers. After all vCenter Servers in the group are upgraded to version 5.0, you can rejoin them.
- Each vCenter Server user sees the vCenter Server instances on which they have valid permissions.
- When you set up your vCenter Server Linked Mode group, you must install the first vCenter Server as a standalone instance because you do not yet have a remote vCenter Server machine to join. Subsequent vCenter Server instances can join the first vCenter Server or other vCenter Server instances that have joined the Linked Mode group.
- If you join a vCenter Server to a standalone instance that is not part of a domain, you must add the standalone instance to a domain and add a domain user as an administrator.
- The vCenter Server instances in a Linked Mode group do not need to have the same domain user login. The instances can run under different domain accounts. By default, they run as the LocalSystem account of the machine on which they are running, which means that they are different accounts.
- During vCenter Server installation, if you enter an IP address for the remote instance of vCenter Server, the installer converts it into a fully qualified domain name.
- You cannot join a Linked Mode group during the upgrade procedure when you are upgrading from VirtualCenter 25 to vCenter Server 5.0. You can join after the upgrade to vCenter Server is complete.

See the *vSphere Upgrade* documentation.



**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 221.

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

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

- Linked Mode groups that contain both vCenter Server 5.0 and earlier versions of vCenter Server are not supported. The vSphere Client does not function correctly with vCenter Servers in groups that have both version 5.0 and earlier versions of vCenter Server. Do not join a version 5.0 vCenter Server to earlier versions of vCenter Server, or an earlier version of vCenter Server to a version 5.0 vCenter Server. Upgrade any vCenter Server instance to version 5.0 before joining it to a version 5.0 vCenter Server.
- To join a Linked Mode group the vCenter Server must be in evaluation mode or licensed as a Standard edition. vCenter Server Foundation and vCenter Server Essentials editions do not support Linked Mode.
- DNS must be operational for Linked Mode replication to work.

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

## 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 5.0. 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 221 .

---

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

---

### 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
<b>Yes, let VMware vCenter Server resolve the conflicts for me</b>	Click <b>Next</b> . The role on the joining system is renamed to <i>vcenter_namerole_name</i> , where <i>vcenter_name</i> is the name of the vCenter Server system that is joining the Linked Mode group, and <i>role_name</i> is the name of the original role.
<b>No, I'll resolve the conflicts myself</b>	To resolve the conflicts manually: <ol style="list-style-type: none"> <li>Using the vSphere Client, log in to one of the vCenter Server systems using an account with <b>Administrator</b> privileges.</li> <li>Rename the conflicting role.</li> <li>Close the vSphere Client session and return to the vCenter Server installer.</li> <li>Click <b>Back</b> and click <b>Next</b>.</li> </ol> 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

- Select **Start > All Programs > VMware > vCenter Server Linked Mode Configuration**.
- Click **Modify linked mode configuration** and click **Next**.
- Click **Isolate this vCenter Server instance from linked mode group** and click **Next**.
- 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 223
- 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 222.

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 226.

### 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>.

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

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

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

If you have a license server installed, you can configure your newly installed or upgraded vCenter Server to use the license server. If you do not have a license server installed, you can download the VMware License Server from the VMware Web site at

[http://downloads.vmware.com/d/details/esx\\_35\\_licenseserver\\_dt/dGViZGV0KmJkZXBo](http://downloads.vmware.com/d/details/esx_35_licenseserver_dt/dGViZGV0KmJkZXBo). After you have installed the license server, configure vCenter Server to use it.

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

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

## 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, open the command prompt in the vCenter Server and change the directory to `vCenter_Server_installation_directory\Infrastructure\Inventory Service\scripts`.
- 2 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.

### What to do next

See [“Restore an Inventory Service Database Backup on Windows,”](#) on page 227.

## 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 VirtualCenter service.
  - a Select **Start > Control Panel > Administrative Tools > Services**.
  - b Right-click **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 command prompt in the vCenter Server and change the directory to `/usr/lib/vmware-vpx/inventoryservice/scripts/`.
- 2 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 228.

## 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.

## Update the vCenter Inventory Service URL Configuration

If the actual host name or domain name of the vCenter Server machine does not match the name that was entered at installation, the service does not work. When the host name or domain name of the vCenter Server machine changes after you install vCenter Server, update the configuration information of the inventory service.

### Procedure

- 1 Stop the vCenter Inventory Service.
  - a From the Windows **Start** menu, select **Administrative Tools > Services**.
  - b Right-click **vCenter Inventory Service** and select **Stop**.
- 2 Open a command prompt.
- 3 Change directory to *Inventory\_Service\_directory/scripts*

The location of the Inventory Service directory is specified during the vCenter Server installation. For example, if you installed vCenter Inventory Service in the default location, run this command.

```
cd /Program Files/VMware/Infrastructure/Inventory Service/scripts
```
- 4 Run the `register.bat` command to update the stored configuration information of the Inventory Service.
 

```
register.bat current_vCenter_Server_fully_qualified_domain_name vCenter_Server_HTTPS_port
```

For example, if the vCenter Server fully qualified domain name is `machinename.corp.com` and the HTTPS port is 443, run this command.

```
register.bat machinename.corp.com 443
```
- 5 Restart the vCenter Inventory Service.
  - a From the Windows **Start** menu, select **Administrative Tools > Services**.
  - b Right-click **vCenter Inventory Service** and select **Start**.

The vCenter Inventory Service URL configuration is updated.

## 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** This procedure can cause data loss. Perform this procedure with VMware Technical Support.

### Procedure

- 1 Stop the vCenter Inventory Service.
  - a From the Windows **Start** menu, select **Administrative Tools > Services**.
  - b Right-click **vCenter Inventory Service** and select **Stop**.
- 2 Open a command prompt.
- 3 Delete the entire contents of the *Inventory\_Service\_Directory/data* directory.
 

The location of the Inventory Service directory is specified during the vCenter Server installation.

- 4 Change directory to *Inventory\_Service\_directory/scripts*

For example, if you installed vCenter Inventory Service in the default location, run this command.

```
cd /Program Files/VMware/Infrastructure/Inventory Service/scripts
```

- 5 Run the `createdb.bat` command, with no arguments, to reset the vCenter Inventory Service database.

- 6 Run the `register.bat` command to update the stored configuration information of the Inventory Service.

```
register.bat current_vCenter_Server_fully_qualified_domain_name vCenter_Server_HTTPS_port
```

For example, if the vCenter Server fully qualified domain name is `machinename.corp.com` and the HTTPS port is 443, run this command.

```
register.bat machinename.corp.com 443
```

- 7 Restart the vCenter Inventory Service.

- a From the Windows **Start** menu, select **Administrative Tools > Services**.

- b Right-click **vCenter Inventory Service** and select **Start**.

The vCenter Inventory Service database is reset.

# Index

## Symbols

%include command **51**  
%post command **51**  
%pre command **51**

## Numerics

3rd-party modules, removing **163**  
64-bit DSN requirement **170**

## A

acceptance levels  
    image profiles **137**  
    VIBs **127**  
acceptance levels, host **136**  
accepteula command **51**  
access, restricting **160**  
active rule set **66**  
Add-DeployRule **120**  
administrative password **148**  
advanced management (Auto Deploy) **92**  
answer file **63, 86, 93**  
answer files **95, 121**  
Apply-EsxImageProfile cmdlet **85**  
Authentication Proxy, *See also* vSphere  
    Authentication Proxy  
Auto deploy, answer file **93**  
Auto Deploy  
    answer files **121**  
    best practices **98**  
    boot file **73**  
    boot operation **63**  
    boot process **67**  
    change target vCenter Server **94**  
    coredump **103**  
    DHCP address **105**  
    DHCP reservations **111**  
    DHCP server **73, 111**  
    DNS Server **113**  
    failing to complete boot **104**  
    failure to boot **106**  
    gPXE boot **117**  
    host profiles **119**  
    image profile warning **103**  
    installation option **14**  
    installing **113**  
    network boot problem **105**  
    networking **91**  
    PowerCLI cmdlets **72**  
    PowerCLI installation **110**  
    PowerCLI setup **110**  
    preparing **73**  
    proof of concept **108**  
    proof of concept checklist **108**  
    provisioning hosts **83**  
    rebooting **84**  
    redirection problem **102**  
    reference host **86, 118**  
    reprovisioning hosts with **84**  
    reregister **92**  
    rule set compliance **82**  
    rules **116**  
    static IP address **93**  
    tasks **70**  
    TFTP server **73, 106**  
    timeout error **101**  
    troubleshooting **101**  
    tutorial **108**  
    user input **84**  
    wrong image **102**  
    *See also* vSphere Auto Deploy  
Auto Deploy daemon **92**  
Auto Deploy image **115**  
Auto Deploy on vCenter Server Appliance **94**  
Auto Deploy PowerCLI **76, 79**  
Auto Deploy PowerCLI cmdlets **66**  
Auto Deploy roadmap **70**  
Auto Deploy rules **80, 81**  
Auto Deploy server **63**  
auto-deploy register command **94**

## B

banner, security **146**  
best practices, Auto Deploy **98**  
BIOS **149**  
BIOS UUID **63**  
boot command line options **49**  
boot commands, entering **48**  
boot disk, shared **158**  
boot failure in UEFI mode. **150**

- boot file (Auto Deploy) **73**
- boot operations **63**
- boot process, Auto Deploy **67**
- boot prompt **49**
- boot setting **149**
- boot.cfg file **58**
- bootloader kernel options **49**
- bulk licensing **77**
- bundled database **171**

## C

- CD-ROM, booting from virtual **149**
- CD/DVD, burning the ESXi ISO image **16**
- clearpart command **51**
- clients, firewall **38, 39**
- cluster location, assign with Auto Deploy **81**
- components included with the vCenter Server installer **205**
- computer name
  - Oracle **171**
  - SQL Server **171**
- configuration defaults, resetting **162**
- configuring a DB2 database **172**
- configuring ports **38, 39**
- configuring the keyboard **146**
- Connect-VIServer cmdlet **79–81, 85**
- connecting
  - Oracle database **194, 195**
  - SQL Server database **188**
- Copy-DeployRule cmdlet **85**
- creating a DB2 database **175**
- creating a SQL Server database **181**
- creating an Oracle database **192**
- custom packages, removing **163**

## D

- data source name **170**
- database corruption, Auto Deploy **107**
- Database Monitoring, enabling for Microsoft SQL Server user **190**
- Database Monitoring, enabling for Oracle user **196**
- database roles, setting vCenter user rights **182**
- databases
  - maintaining **171**
  - Oracle **194**
  - preparing **221**
  - SQL Server **188, 189**
- DB2, creating the schema **176**
- DB2 database
  - client instance registry variables **174**
  - configure for remote connection **178, 179**
  - configure locally on Microsoft Windows **178**

- database instance registry variables **173**
  - script for creating **175**
  - user and group **172**
- DB2 database configuration **172**
- DBO privileges **181**
- deactivating ESXi **163**
- default installation scripts **50**
- default root password **50**
- default storage behavior **156**
- defaults, restoring **162**
- depots **138**
- DHCP
  - direct console **153, 154**
  - for PXE booting the ESXi installer **21**
  - vSphere Client **153**
- DHCP reservations, Auto Deploy **111**
- DHCP Scope **111**
- DHCP Server, Auto Deploy **111**
- DHCP server for Auto Deploy **73**
- direct console
  - boot setting **149**
  - configuring the keyboard **146**
  - DHCP **153, 154**
  - DNS **154**
  - IP addressing **153, 154**
  - management network **150–152**
  - navigating **146**
  - network adapters **152**
  - network settings **150–152**
  - password configuration **148**
  - redirecting by setting the boot options **147**
  - redirecting to a serial port **147**
  - security banner **146**
  - static addressing **153, 154**
  - testing management network **154, 156**
  - VLAN ID **152**
- direct console, redirecting to a serial port in an Auto Deploy host **148**
- Directory Services **222, 223**
- disabling the management network **155**
- Distributed Switch, See vSphere Distributed Switch
- DNS **153, 154, 225**
- DNS Requirements **40**
- DNS Server, Auto Deploy **113**
- DNS suffixes, direct console **154**
- domain controller **225**
- Download TFTP ZIP **73**
- download the vCenter Server installer **206**
- DRAC **41**
- dryrun command **51**
- DSN, 64-bit requirement **170**



Dump Collector, *See* vSphere ESXi Dump Collector

## E

esxcli system coredump **88**

ESXi

about **145**

deactivating **163**

installation options **14**

installing **43**

installing interactively **43**

managing remotely **151**

syslog service **159**

system requirements **29**

ESXi Dump Collector

host profiles **90**

reference host **90**

ESXi Image Builder CLI, customized ESXi

installation images **15**

ESXi installation, required information **26**

ESXi installation script, about **50**

ESXi ISO image, burning on a CD/DVD **16**

ESXi setup, post-setup **165**

ESXi Shell access to host **161**

ESXi, convert to evaluation mode **166**

evaluation mode **15, 166**

## F

factory defaults, restoring **162**

firewall

network-based **226**

Windows **225**

floppy, booting from virtual **149**

folder location, assign with Auto Deploy **81**

FTP **19**

## G

Get-Help PowerShell cmdlet **76**

global data **222, 223**

gpupdate /force command **225**

gPXE **19**

group policy update **225**

groups, requirements **221**

guest operating systems **32**

GUID **225**

## H

hardware requirements

ESXi **29**

vCenter Server **33**

vCenter Server Appliance **33**

hardware requirements, ESXi **31**

host image profile acceptance level **161**

host profile from reference host **118**

host profiles

assign with Auto Deploy **80**

Auto Deploy **89**

Auto Deploy rule **120**

Network Coredump **89**

reference host for Auto Deploy **118**

host provisioning **63**

host settings, preserving during ESXi

installation **13**

hosts, reprovisioning with Auto Deploy **84**

hosts firewall **38, 39**

## I

IBM DB2, requirements **169**

IDE disks **29, 31**

IIS, conflict with vCenter Server over port 80 **40**

ILO **41**

Image Builder

and Auto Deploy **123**

overview **123**

*See also* ESXi Image Builder CLI

Image Builder CLI, *See* vSphere ESXi Image Builder CLI

Image Builder sessions **135**

Image Builder, installing **130**

Image Builder, workflows **138**

image profile **115**

image profiles

acceptance level **137**

editing **142**

Image profiles, cloning **131**

Image profiles, creating **131, 140**

image profiles, export **133**

image profiles, validation **126**

ImageProfile structure **127**

include command **51**

install command **51**

Installation overview **13**

installation script

customized in ISO image **18**

path to **51**

supported locations **50**

installation script, creating **47**

installation scripts, default **50**

installing

ESXi **43**

Update Manager server **214**

vCenter Server **206**

vCenter Server in a virtual machine **208**

VirtualCenter Server **221**

VMware vSphere Web Client **213**

vSphere Client **212**

installing ESXi, scripted **47**

- installing ESXi interactively **43**
- installorupgrade command **51**
- interactive installation **14**
- Inventory Service, *See also* vCenter Inventory Service
- Inventory Service database
  - back up on Linux **228**
  - back up on Windows **227**
  - restore on Linux **228**
  - restore on Windows **227**
- IP, on a detached host **150, 151**
- IP address, vCenter Server with multiple network interfaces **224**
- IP addressing
  - direct console **153, 154**
  - vSphere Client **153**
- IPv6 **200**
- IPv6 address, format **200**
- iSCSI software disk, installing ESXi on **45**
- ISO
  - create **133**
  - export **133**
- ISO image, with custom installation script **18**

## J

- JDBC **189**
- JDBC URL formats **200**
- JVM heap settings, recommended for vCenter Virtual Appliance **33**

## K

- keyboard command **51**
- keyboard, localizing **146**
- kickstart commands **58**
- kickstart file, creating **47**
- ks.cfg **50**

## L

- LDAP **222**
- license key **166, 167**
- license server, managing legacy hosts **226**
- licensed mode **15, 166**
- LicenseDataManager **77**
- licensing, bulk licensing **77**
- licensing ESXi hosts **165**
- Linked Mode
  - and databases **221**
  - and permissions **221**
  - reachability **201, 224, 225**
  - requirements **221**
  - troubleshooting **225, 226**
- local Oracle database **194, 195**
- local SQL Server database **181**

- localizing, keyboard **146**
- lockdown mode **160**
- logging, providing space for **37**
- logical volume management **156**
- LVM **156**

## M

- MAC address **22, 63**
- maintaining the database **171**
- management agents, restarting **154**
- management network
  - direct console **150–152**
  - disabling **155**
  - restarting **155**
  - testing **154, 156**
- media options, ESXi installer, supported **15**
- memory, ESXi requirements **29, 31**
- message, security **146**
- Microsoft .NET **76, 130**
- Microsoft .NET Framework **37, 205**
- Microsoft PowerShell **76, 130**
- Microsoft SQL database permissions, setting by
  - using the dbo schema and db\_owner database role **183**
- Microsoft SQL Native Client **171**
- Microsoft SQL Server, requirements **169**
- Microsoft SQL Server 2008 R2 Express **171, 205**
- Microsoft SQL Server database schema, creating
  - with a script (recommended method) **184**
- Microsoft Windows
  - authentication for SQL Server **199**
  - system account **199**
- Microsoft Windows Installer **205**

## N

- navigating, direct console **146**
- network adapters, direct console **152**
- network boot **110**
- network command **22, 51**
- network core dump **88**
- network drive, installing from **202**
- network settings, direct console **150–152**
- New-DeployRule **116, 120**
- New-DeployRule cmdlet **79–81**
- New-EsxImageProfile cmdlet **131**
- NewEsxImageProfile cmdlet **140**
- non-ASCII characters, disable support for **163**

**O**

ODBC databases **188**

offline bundle

create **133**

export **133**

Oracle database

changing the computer name **171**

remote access **194**

requirements **169**

script for creating **192**

user **191**

Oracle database schema **192**

Oracle, preparing database **194**

**P**

paranoid command **51**

part command **51**

partition command **51**

partitions **156, 157**

password, administrative **148**

plug-ins for vCenter Server **212**

port 80 conflict between vCenter Server and IIS **40**

ports

configuring **38, 39**

firewall **38, 39**

ports used by vCenter Server **38**

ports used by vCenter Server Appliance **39**

PowerCLI **79**

PowerCLI cmdlets, Auto Deploy **72**

PowerCLI sessions **135**

PowerCLI wildcard characters **138**

Preface **7**

preinstallation checklist **108**

preparing database **195**

prerequisites for installing vCenter Server **197**

PXE, configuration files **22**

PXE boot ESXi installer using PXELINUX, setup procedure **22, 24, 25**

PXELINUX

boot ESXi installer using **22, 25**

boot ESXi installer using **24**

**R**

redirecting log files **159**

reference host

Auto Deploy **89**

configuration options **88**

reference host for Auto Deploy **86**

registration of Auto Deploy **92**

registry settings **225, 226**

reinstalling vCenter Server **220**

remote access, restricting **160**

remote management applications **26**

remote management of ESXi **151**

remote Oracle database **194**

remote SQL Server database **181**

removing 3rd-party modules **163**

removing custom packages **163**

removing vCenter Server **220**

Repair-DeployRulesetCompliance cmdlet **82**

requirements for vSphere Client **37**

requirements for vSphere Web Client **37**

resetting configuration defaults **162**

restarting the management agents **154**

restarting the management network **155**

restoring, factory defaults **162**

restricting access **160**

ROM image **19**

root access, restricting **160**

root password **148**

rootpw command **51**

RPCCfg.exe **225, 226**

RSA **41**

rule engine **66**

rule set **63**

rule set compliance **82**

rule sets **66**

rules **66, 120**

**S**

SAS disks **29, 31**

SATA disks **29, 31**

schema, for DB2 **176**

scratch partition, enabling **158**

scratch storage **156, 157**

script, for installing ESXi **50**

script for DB2 database **175**

script for Oracle database **192**

script for SQL Server database **181**

scripted database schema creation, for DB2 **176**

scripted installation, differences from ESXi 4.x **57**

scripted installation of ESXi, by PXE Booting **61**

scripted installation of ESXi, from a USB flash drive **60**

scripted installation of ESXi, from a CD or DVD **59**

scripted installation option **14**

SCSI **29, 31**

SDK **201, 224, 225**

security **199**

security banner **146**

- serial port
  - redirecting the direct console to **147**
  - redirecting the direct console using the vSphere Client **147**
- Service Console, removed in ESXi 5.0 **11**
- services, syslogd **159**
- sessions, PowerCLI **135**
- SMBIOS information **63**
- snap-in, Auto Deploy **76**
- software depot **115**
- software depots, examining **138**
- SoftwarePackage structure **127**
- specifications
  - ESXi hardware requirements **29, 31**
  - performance recommendations **29, 31**
- SQL compatibility mode **204**
- SQL Server
  - changing the computer name **171**
  - Microsoft Windows authentication **199**
  - preparing the database **188, 189**
  - script for creating **181**
- SSH access to host **161**
- Standard switch, restoring **155**
- starting the vSphere Client **213**
- state **63**
- static addressing, about **150–152**
- static DNS **153**
- static DNS, direct console **154**
- static IP **153**
- static IP address for Auto Deploy **93**
- storage **156**
- subnet mask **153**
- support information **166, 167**
- syslog, host profile **91**
- Syslog Collector, *See* vSphere Syslog Collector
- syslog, Auto Deploy **91**
- system requirements, vCenter Server
  - database **169**
- system swap **156, 157**

## T

- target hosts **110**
- TCP/IP setup for SQL Server **189**
- template host for Auto Deploy **86**
- Test-DeployRuleSetCompliance cmdlet **82**
- testing management network, direct console **156**
- TFTP **19**
- TFTP Boot ZIP **114**
- TFTP server
  - Auto Deploy **106**
  - installing **109**
- TFTP server for Auto Deploy **73**

- tftp-hpa **19**
- tftpd32 **19**
- timeout error, Auto Deploy **101**
- troubleshooting, Linked Mode **224, 225**
- troubleshooting for Linked Mode **201**

## U

- UEFI mode, ESXi fails to boot **150**
- uninstalling vCenter Server **220**
- unregister Auto Deploy **94**
- updated information **9**
- upgrade command **51**
- upgrading ESXi, scripted **47**
- URLs, configuring **201, 224**
- USB, bootable ESXi installation **16**
- USB, ESXi installation script **17**
- user and group for DB2 database **172**
- user and group for Oracle database **191**
- user input for Auto Deploy **86**
- user input for Auto Deploy hosts **84**

## V

- vCenter Inventory Service, updating URL **229**
- vCenter Orchestrator **205**
- vCenter Server
  - additional components **212**
  - before you install **197**
  - components **205**
  - configuring URLs **201, 224**
  - DB2 database (local) **178**
  - DB2 database (remote) **178, 179**
  - downloading the installer **206**
  - hardware requirements **33**
  - install procedure **206**
  - installing **205**
  - installing from a network drive **202**
  - installing in a virtual machine **208**
  - installing on IPv6 machine **200**
  - joining a group **222, 223**
  - Linked Mode **220**
  - plug-ins **212**
  - ports **38**
  - prerequisites for installing **197**
  - required information for installation **202**
  - required information for vCenter Server installation **202**
  - requirements for joining a group **221**
  - setting user rights through database roles **182**
  - software requirements **36**
  - system requirements **29**
- vCenter Server Appliance
  - Auto Deploy **93, 94**

- ports **39**
  - See also* VMware vCenter Server Appliance
  - vCenter Server Appliance:Auto Deploy **93, 94**
  - vCenter Server database
    - Microsoft SQL Server **180**
    - Oracle **190**
  - vCenter Server databases, preparing **169**
  - vCenter Server installation, post-installation **211**
  - vCenter Server installed as local system
    - account **199**
  - vCenter Server MSSQL database objects,
    - creating manually with a script **185**
  - vCenter Virtual Appliance, JVM heap settings **33**
  - vCenterServer.VimApiUrl **201, 224**
  - vCenterServer.VimWebServicesUrl **201, 224**
  - VIB, third party **123**
  - VIB structure **127**
  - VIBs **123, 124**
  - VIBs, acceptance levels **127**
  - VIBs, validation **126**
  - viewing, log files **159**
  - virtual CD **26**
  - virtual machine, installing vCenter Server in **208**
  - virtual machines, RAM requirements **29, 31**
  - virtual media **149**
  - VirtualCenter Management Webservices **211**
  - VLAN ID, direct console **152**
  - vmaccepteula command **51**
  - VMFS **156**
  - VMFS datastore, preserving during ESXi
    - installation **13**
  - vmk0 **91**
  - vmkernel module, removing **163**
  - VMware vCenter Management
    - Webservices **226**
  - VMware vCenter Server Appliance
    - downloading and deploying **209**
    - hardware requirements **33**
    - software requirements **36**
  - VMware vSphere Web Client, installing and
    - starting **213**
  - vmware-fdm package **102**
  - vmware-rbd-watchdog **94**
  - vSphere 5.0, changes from vSphere 4.x.x **11**
  - vSphere Authentication Proxy
    - IIS installation causes port 80 conflict **40**
    - installing **218**
  - vSphere Auto Deploy
    - installing **218**
    - installing ESXi with **63**
  - vSphere CLI **158**
  - vSphere Client
    - DHCP **153**
    - downloading **212**
    - hardware requirements **33**
    - installing **212**
    - installing from a network drive **202**
    - managing ESXi host **165**
    - requirements **37**
    - starting **213**
    - static addressing **153**
  - vSphere Distributed Switch, restoring standard
    - switch **155**
  - vSphere ESXi Dump Collector, installing **216**
  - vSphere ESXi Image Builder CLI, using **123**
  - vSphere HA, Auto Deploy **102**
  - vSphere installation and setup, introduction **11**
  - vSphere Syslog Collector, installing **217**
  - vSphere Update Manager **205**
  - vSphere Update Manager,databases **169**
  - vSphere Web Client
    - hardware requirements **33**
    - managing ESXi host **165**
    - requirements **37**
    - See also* VMware vSphere Web Client
  - vSwitch0 **91**
  - VWS **201, 224, 225**
- ## W
- waiter.tgz file **101**
  - web client, *See* VMware vSphere Web Client
  - wildcard characters, PowerCLI **138**
  - working rule set **66**

