vSphere Installation and Setup

vSphere 6.0

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

EN-001667-03

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About vSphere Installation and Setup

vSphere Installation and Setup describes how to install and configure VMware® vCenter Server, deploy the vCenter Server Appliance, and ESXi.

Intended Audience

vSphere Installation and Setup is intended for experienced administrators who want to install and configure vCenter Server, deploy and configure the vCenter Server Appliance, and install and configure ESXi.

This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. The information about using the Image Builder and Auto Deploy is written for administrators who have experience with Microsoft PowerShell and PowerCLI.

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
EN-001667-03	■ Updated "Create a SQL Server Database and User for vCenter Server," on page 188 to edit the example script by changing the location for creating the database and user. ■ Updated "Synchronize ESXi Clocks with a Network Time Server," on page 209 to state that you must connect to vCenter Server by using the vSphere Client. ■ Updated "Download the vCenter Server Appliance Installer," on page 234 to add information about mounting an ISO image to a virtual machine.
EN-001667-02	■ Updated "Repointing the Connections Between vCenter Server and Platform Services Controller," on page 252 to correct the syntax of the `vmafd-cli set-dc-name` and `vmafd-cli set-dc-port` commands. ■ Updated "Auto Deploy Best Practices," on page 112 to remove the information that vCenter Server Heartbeat can be deployed and used for High Availability. With vSphere 6.0 vCenter Server Heartbeat is discontinued.

Revision	Description
EN-001667-01	■ Updated topics "vCenter Server Deployment Models," on page 13, "Enhanced Linked Mode Overview," on page 20, "Install vCenter Server with an Embedded Platform Services Controller," on page 224, and "Deploy the vCenter Server Appliance with an Embedded Platform Services Controller," on page 235 with information about the recommended topologies. ■ Updated topics "vCenter Server for Windows Hardware Requirements," on page 30 and "vCenter Server Appliance Hardware Requirements," on page 31 with information about the hardware requirements for the embedded deployment models. ■ Updated the information in topics Chapter 1, "Introduction to vSphere Installation and Setup," on page 11, "vCenter Server Appliance Requirements," on page 31, "vCenter Server Appliance Software Requirements," on page 33, and Chapter 7, "Before You Install vCenter Server or Deploy the vCenter Server Appliance," on page 185 to state that the vCenter Server Appliance can be deployed on hosts running ESXi 5.0 or later. ■ Updated topics "Configure a SQL Server ODBC Connection," on page 195 and "Using a User Account for Running vCenter Server," on page 209 with information about using a SQL Server database when the vCenter Server service is running under the Windows built-in system account. ■ Updated the information in topics "Deploy the vCenter Server Appliance with an Embedded Platform Services Controller," on page 235, "Deploy a Platform Services Controller Appliance," on page 238, and "Deploy the vCenter Server Appliance," on page 240 to state that for the network configurations, non-ephemeral distributed virtual port groups are not supported and are not displayed in the **Choose a network** drop-down menu. ■ Added a new step in topic "Repointing the Connections Between vCenter Server and Platform Services Controller," on page 252 that is necessary only if Platform Services Controller B uses an HTTPS port number different from the HTTPS port used by Platform Services Controller A. ■ Updated the Chapter 12, "Backing Up and Restoring vCenter Server," on page 255 chapter with information that this section is only about embedded deployment models. ■ Added information in topic Chapter 12, "Backing Up and Restoring vCenter Server," on page 255 that restoring virtual machines that have snapshots is unsupported.
EN-001667-00	Initial release.

Introduction to vSphere Installation and Setup 1

vSphere 6.0 provides various options for installation and setup. To ensure a successful vSphere deployment, understand the installation and setup options, and the sequence of tasks.

The two core components of vSphere are VMware ESXi® and VMware vCenter Server®. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. vCenter Server lets you pool and manage the resources of multiple hosts.

You can install vCenter Server on a Windows virtual machine or physical server, or deploy the vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy the vCenter Server Appliance on hosts running ESXi 5.0 or later.

Starting with vSphere 6.0, all prerequisite services for running vCenter Server and the vCenter Server components are bundled in the VMware Platform Services Controller. You can deploy vCenter Server with an embedded or external Platform Services Controller, but you must always install or deploy the Platform Services Controller before installing or deploying vCenter Server.

This chapter includes the following topics:

vCenter Server Components and Services

vCenter Server provides a centralized platform for management, operation, resource provisioning, and performance evaluation of virtual machines and hosts.

When you install vCenter Server with an embedded Platform Services Controller, or deploy the vCenter Server Appliance with an embedded Platform Services Controller, vCenter Server, the vCenter Server components, and the services included in the Platform Services Controller are deployed on the same system.

When you install vCenter Server with an external Platform Services Controller, or deploy the vCenter Server Appliance with an external Platform Services Controller, vCenter Server and the vCenter Server components are deployed on one system, and the services included in the Platform Services Controller are deployed on another system.

The following components are included in the vCenter Server and vCenter Server Appliance installations:

- The VMware Platform Services Controller group of infrastructure services contains vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority.
- The vCenter Server group of services contains vCenter Server, vSphere Web Client, Inventory Service, vSphere Auto Deploy, vSphere ESXi Dump Collector, VMware vSphere Syslog Collector on Windows and VMware Sphere Syslog Service for the vCenter Server Appliance.

Services Installed with VMware Platform Services Controller

vCenter Single Sign-On

The vCenter Single Sign-On authentication service provides secure authentication services to the vSphere software components. By using vCenter Single Sign-On, the vSphere components communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. vCenter Single Sign-On constructs an internal security domain (for example, vsphere.local) where the vSphere solutions and components are registered during the installation or upgrade process, providing an infrastructure resource. vCenter Single Sign-On can authenticate users from its own internal users and groups, or it can connect to trusted external directory services such as Microsoft Active Directory. Authenticated users can then be assigned registered solution-based permissions or roles within a vSphere environment.

vCenter Single Sign-On is available and required with vCenter Server 5.1.x and later.

vSphere License Service

The vSphere License service provides common license inventory and management capabilities to all vCenter Server systems that are connected to a Platform Services Controller or multiple linked Platform Services Controllers.

VMware Certificate Authority

VMware Certificate Authority (VMCA) provisions each ESXi host with a signed certificate that has VMCA as the root certificate authority, by default. Provisioning occurs when the ESXi host is added to vCenter Server explicitly or as part of the ESXi host installation process. All ESXi certificates are stored locally on the host.

Services Installed with vCenter Server

These additional components are installed silently when you install vCenter Server. The components cannot be installed separately as they do not have their own installers.

vCenter Inventory Service

Inventory Service stores vCenter Server configuration and inventory data, enabling you to search and access inventory objects across vCenter Server instances.

PostgreSQL

A bundled version of the VMware distribution of PostgreSQL database for vSphere and vCloud Hybrid Services.

vSphere Web Client

The vSphere Web Client lets you connect to vCenter Server instances by using a Web browser, so that you can manage your vSphere infrastructure.

vSphere ESXi Dump Collector

The vCenter Server support tool. You can configure ESXi to save the VMkernel memory to a network server, rather than to a disk, when the system encounters a critical failure. The vSphere ESXi Dump Collector collects such memory dumps over the network.

VMware vSphere Syslog Collector

The vCenter Server on Windows support tool that enables network logging and combining of logs from multiple hosts. You can use the vSphere Syslog Collector to direct ESXi system logs to a server on the network, rather than to a local disk. The recommended maximum number of supported hosts to collect logs from is 30. For information about configuring vSphere Syslog Collector, see http://kb.vmware.com/kb/2021652.

VMware Syslog Service

The vCenter Server Appliance support tool that provides a unified architecture for system logging, network logging and collecting logs from hosts. You can use the VMware Syslog Service to direct ESXi system logs to a server on the network, rather than to a local disk. The recommended maximum number of supported hosts to collect logs from is 30. For information about configuring VMware Syslog Service, see *vCenter Server Appliance Configuration*.

vSphere Auto Deploy

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

vCenter Server Deployment Models

You can install vCenter Server on a virtual machine or a physical server running Microsoft Windows Server 2008 SP2 or later, or can deploy the vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine, optimized for running vCenter Server.

vSphere 6.0 introduces vCenter Server with an embedded Platform Services Controller and vCenter Server with an external Platform Services Controller.

IMPORTANT This documentation provides information about the basic deployment models. For information about the recommended topologies, see List of recommended topologies for vSphere 6.0.x.

vCenter Server with an embedded Platform Services Controller

All services bundled with the Platform Services Controller are deployed on the same virtual machine or physical server as vCenter Server.

vCenter Server with an external Platform Services Controller

The services bundled with the Platform Services Controller and vCenter Server are deployed on different virtual machines or physical servers.

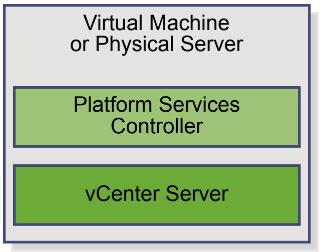
You first must deploy the Platform Services Controller on one virtual machine or physical server and then deploy vCenter Server on another virtual machine or physical server.

IMPORTANT You cannot switch the models after deployment, which means that after you deploy vCenter Server with an embedded Platform Services Controller, you cannot switch to vCenter Server with an external Platform Services Controller, and the reverse.

vCenter Server with an Embedded Platform Services Controller

vCenter Server and the Platform Services Controller are deployed on a single virtual machine or physical server.

Figure 1-1. vCenter Server with an Embedded Platform Services Controller



Installing vCenter Server with an embedded Platform Services Controller has the following advantages:

- The connection between vCenter Server and the Platform Services Controller is not over the network, and vCenter Server is not prone to outages because of connectivity and name resolution issues between vCenter Server and the Platform Services Controller.
- If you install vCenter Server on Windows virtual machines or physical servers, you will need fewer Windows licenses.
- You will have to manage fewer virtual machines or physical servers.
- You do not need a load balancer to distribute the load across Platform Services Controller.

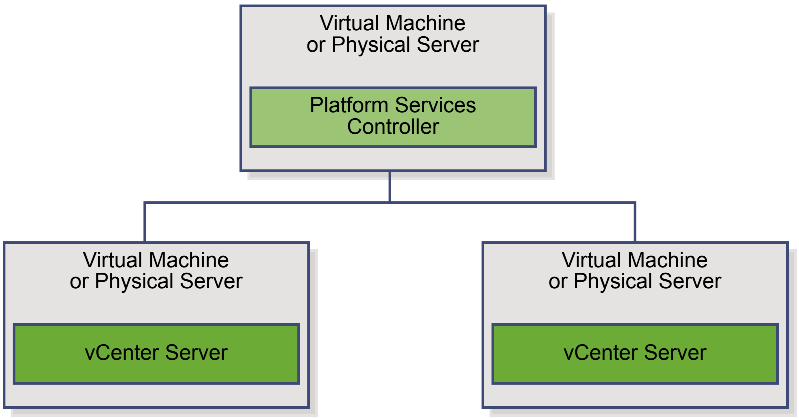
Installing with an embedded Platform Services Controller has the following disadvantages:

- There is a Platform Services Controller for each product which might be more than required. This consumes more resources.
- The model is suitable for small-scale environments.

vCenter Server with an External Platform Services Controller

vCenter Server and the Platform Services Controller are deployed on separate virtual machine or physical server. The Platform Services Controller can be shared across several vCenter Server instances. You can install a Platform Services Controller and then install several vCenter Server instances and register them with the Platform Services Controller. You can then install another Platform Services Controller, configure it to replicate data with the first Platform Services Controller, and then install vCenter Server instances and register them with the second Platform Services Controller.

Figure 1-2. vCenter Server with an External Platform Services Controller



Installing vCenter Server with an external Platform Services Controller has the following advantages:

- Less resources consumed by the combined services in the Platform Services Controllers enables a reduced footprint and reduced maintenance.
- Your environment can consist of more vCenter Server instances.

Installing vCenter Server with an external Platform Services Controller has the following disadvantages:

- The connection between vCenter Server and Platform Services Controller is over the network and is prone to connectivity and name resolution issues.
- If you install vCenter Server on Windows virtual machines or physical servers, you need more Microsoft Windows licenses.
- You must manage more virtual machines or physical servers.

Mixed Operating Systems Environment

A vCenter Server instance installed on Windows can be registered with either a Platform Services Controller installed on Windows or a Platform Services Controller appliance. A vCenter Server Appliance, can be registered with either a Platform Services Controller installed on Windows or a Platform Services Controller appliance. Both vCenter Server and the vCenter Server Appliance can be registered with the same Platform Services Controller within a domain.

Figure 1-3. Example of a Mixed Operating Systems Environment with an External Platform Services Controller on Windows

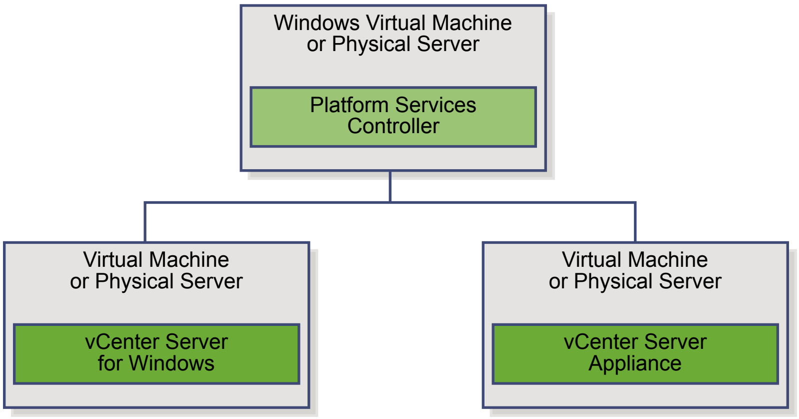
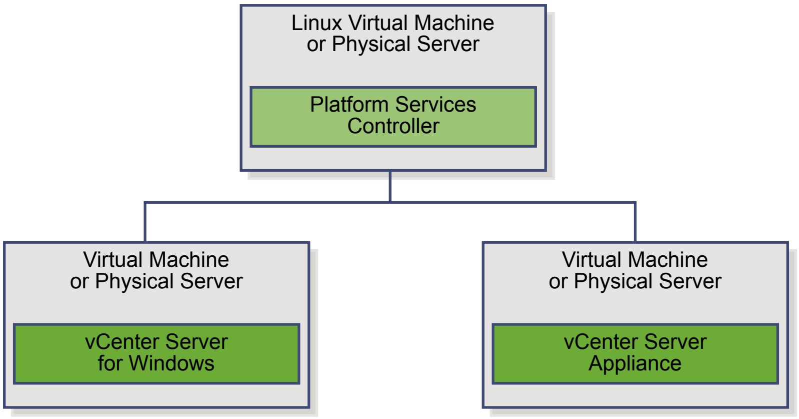

Windows Virtual Machine or Physical Server
Platform Services Controller
Virtual Machine or Physical Server
vCenter Server for Windows
Virtual Machine or Physical Server
vCenter Server Appliance

Figure 1-4. Example of a Mixed Operating Systems Environment with an External Platform Services Controller Appliance


Linux Virtual Machine or Physical Server
Platform Services Controller
Virtual Machine or Physical Server
vCenter Server for Windows
Virtual Machine or Physical Server
vCenter Server Appliance

Having many Platform Services Controllers that replicate their infrastructure data, allows you to ensure high availability of your system.

If an external Platform Services Controller with which your vCenter Server instance or vCenter Server Appliance was initially registered, stops responding, you can repoint your vCenter Server or vCenter Server Appliance to another external Platform Services Controller in the domain. For more information, see "Repointing the Connections Between vCenter Server and Platform Services Controller," on page 252.

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. Read the vSphere release notes.
2. Verify that your system meets vSphere hardware and software requirements. See Chapter 2, "System Requirements," on page 23.
3. Install ESXi.

   a. Verify that your system meets the minimum hardware requirements. See "ESXi Requirements," on page 23.

   b. Determine the ESXi installation option to use. See "Options for Installing ESXi," on page 39.

   c. Determine where you want to locate and boot the ESXi installer. See "Media Options for Booting the ESXi Installer," on page 42. 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 46.

   d. Create a worksheet with the information you will need when you install ESXi. See "Required Information for ESXi Installation," on page 53.

   e. Install ESXi.

      - "Installing ESXi Interactively," on page 55
      - "Installing or Upgrading Hosts by Using a Script," on page 58
      - "Installing ESXi Using vSphere Auto Deploy," on page 71

      IMPORTANT In vSphere 6.0, Auto Deploy is installed together with vCenter Server. To provision ESXi hosts by using Auto Deploy, you must install vCenter Server or deploy the vCenter Server Appliance.

4. Configure ESXi boot and network settings, the direct console, and other settings. See Chapter 5, "Setting Up ESXi," on page 161 and Chapter 6, "After You Install and Set Up ESXi," on page 181.
5. 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. See "Required Free Space for System Logging," on page 38 and "Configure Syslog on ESXi Hosts," on page 176.
6. Install vCenter Server on a Windows virtual machine or physical server or deploy the vCenter Server Appliance.

   In vSphere 6.0, you can install vCenter Server or deploy the vCenter Server Appliance, and connect them in Enhanced Linked Mode configuration by registering the vCenter Server instance and the vCenter Server Appliance to Platform Services Controllers that replicate their infrastructure data.

   Concurrent installations are not supported. After you install or deploy a Platform Services Controller, you must install vCenter Server instances or deploy vCenter Server Appliance sequentially.

   - Install vCenter Server on a Windows virtual machine or physical server.

     1. Verify that your system meets the hardware and software requirements for installing vCenter Server. See "vCenter Server for Windows Requirements," on page 29.
     2. (Optional) Set up an external vCenter Server database. See "Preparing vCenter Server Databases," on page 185.

        For an environment with up to 20 hosts and 200 virtual machines, you can use the bundled PostgreSQL database. For production and large scale environments, set up an external database, because the migration from the embedded PostgreSQL database to an external database is not a trivial manual process.

    3. Create a worksheet with the information you need for installation. See "Required Information for Installing vCenter Server," on page 210.
    4. Install vCenter Server and the Platform Services Controller. See Chapter 8, "Installing vCenter Server on a Windows Virtual Machine or Physical Server," on page 223.

       You can install vCenter Server with an embedded or with an external Platform Services Controller.

       vCenter Server with an embedded Platform Services Controller deployment is suitable for small-scale environments. vCenter Server with an external Platform Services Controller deployment is suitable for environments with several vCenter Server instances. See "vCenter Server Deployment Models," on page 13 .

- Deploy the vCenter Server Appliance.
    1. Review the topics in "vCenter Server Appliance Requirements," on page 31 and verify that your system meets the hardware and software requirements for deploying the vCenter Server Appliance.
    2. (Optional) Set up an external Oracle database. The vCenter Server Appliance supports only Oracle database as an external database. See "Preparing vCenter Server Databases," on page 185.

       You can also use the bundled PostgreSQL database, which is suitable for environments that contain up to 1,000 hosts and 10,000 virtual machines.

    3. Use the topic "Required Information for Deploying the vCenter Server Appliance," on page 214 to create a worksheet with the information you need for installation.
    4. Deploy the vCenter Server Appliance with an embedded Platform Services Controller or with an external Platform Services Controller. See Chapter 9, "Deploying the vCenter Server Appliance," on page 233.

       vCenter Server with an embedded Platform Services Controller deployment is suitable for small-scale environments. vCenter Server with an external Platform Services Controller deployment is suitable for environments with several vCenter Server instances. See "vCenter Server Deployment Models," on page 13 .

7. Connect to vCenter Server from the vSphere Web Client. See Chapter 11, "After You Install vCenter Server or Deploy the vCenter Server Appliance," on page 249.
8. Configure vCenter Server and the vCenter Server Appliance. See *vCenter Server and Host Management* and *vCenter Server Appliance Configuration*.

vSphere Security Certificates Overview

ESXi hosts and vCenter Server communicate securely over SSL to ensure confidentiality, data integrity and authentication.

In vSphere 6.0, the VMware Certificate Authority (VMCA) provisions each ESXi host with a signed certificate that has VMCA as the root certificate authority, by default. Provisioning happens when the ESXi host is added to vCenter Server explicitly or as part of the ESXi host installation. All ESXi certificates are stored locally on the host.

You can also use custom certificates with a different root Certificate Authority (CA). For information about managing certificates for ESXi hosts, see the *vSphere Security* documentation.

All certificates for vCenter Server and the vCenter Server services are stored in the VMware Endpoint Certificate Store (VECS).

You can replace the VMCA certificate for vCenter Server with a different certificate signed by a CA. If you want to use a third party certificate, install the Platform Services Controller, add the new CA-signed root certificate to VMCA, and then install vCenter Server. For information about managing vCenter Server certificates, see the *vSphere Security* documentation.

Certificate Replacement Overview

You can perform different types of certificate replacement depending on company policy and requirements for the system that you are configuring. You can perform each replacement with the vSphere Certificate Manager utility or manually by using the CLIs included with your installation.

VMCA is included in each Platform Services Controller and in each embedded deployment. VMCA provisions each node, each vCenter Server solution user, and each ESXi host with a certificate that is signed by VMCA as the certificate authority. vCenter Server solution users are groups of vCenter Server services. See *vSphere Security* for a list of solution users.

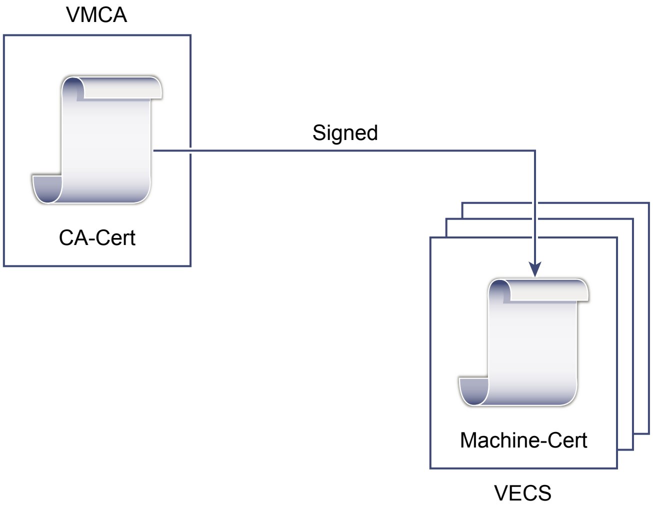
You can replace the default certificates. For vCenter Server components, you can use a set of command-line tools included in your installation. You have several options.

See the *vSphere Security* publication for details on the replacement workflows and on the vSphere Certificate Manager utility.

Replace With Certificates Signed by VMCA

If your VMCA certificate expires or you want to replace it for other reasons, you can use the certificate management CLIs to perform that process. By default, the VMCA root certificate expires after ten years, and all certificates that VMCA signs expire when the root certificate expires, that is, after a maximum of ten years.

Figure 1-5. Certificates Signed by VMCA Are Stored in VECS

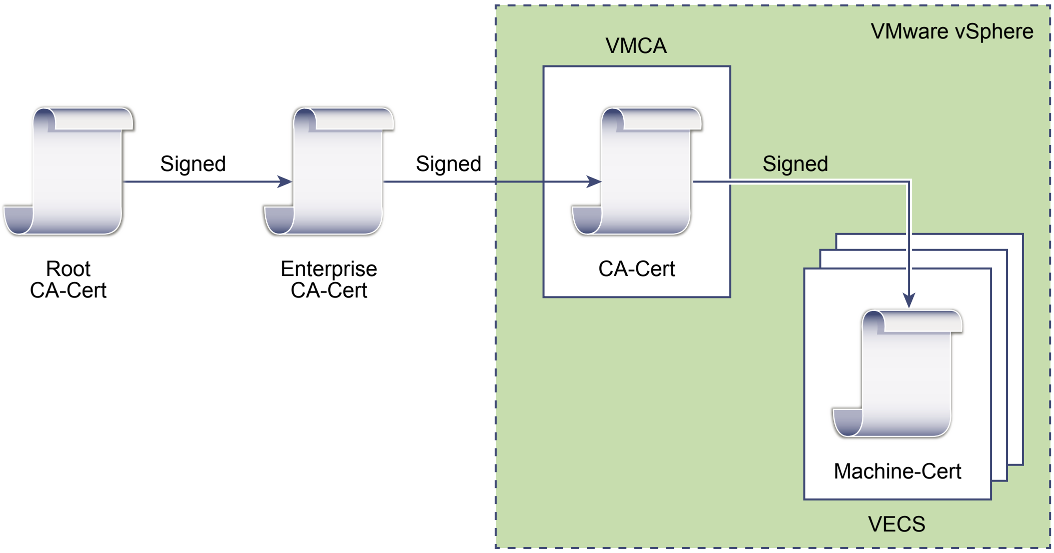


Make VMCA an Intermediate CA

You can replace the VMCA root certificate with a certificate that is signed by an enterprise CA or third-party CA. VMCA signs the custom root certificate each time it provisions certificates, making VMCA an intermediate CA.

Note If you perform a fresh install that includes an external Platform Services Controller, install the Platform Services Controller first and replace the VMCA root certificate. Next, install other services or add ESXi hosts to your environment. If you perform a fresh install with an embedded Platform Services Controller, replace the VMCA root certificate before you add ESXi hosts. If you do, all certificates are signed by the whole chain, and you do not have to generate new certificates.

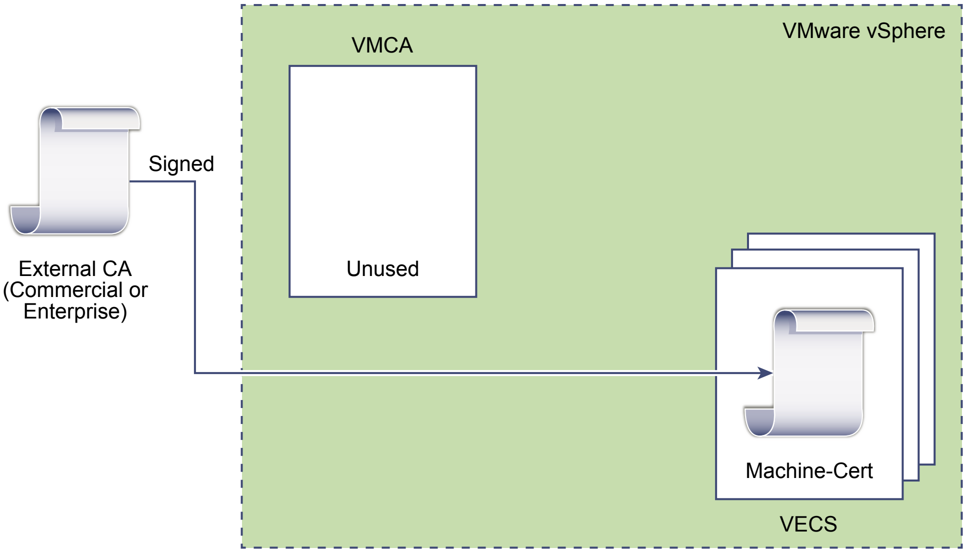
Figure 1-6. Certificates Signed by a Third-Party or Enterprise CA Use VMCA as an Intermediate CA



Do Not Use VMCA, Provision with Custom Certificates

You can replace the existing VMCA-signed certificates with custom certificates. If you use that approach, you are responsible for all certificate provisioning and monitoring.

Figure 1-7. External Certificates are Stored Directly in VECS



Hybrid Deployment

You can have VMCA supply some of the certificates, but use custom certificates for other parts of your infrastructure. For example, because solution user certificates are used only to authenticate to vCenter Single Sign-On, consider having VMCA provision those certificates. Replace the machine SSL certificates with custom certificates to secure all SSL traffic.

ESXi Certificate Replacement

For ESXi hosts, you can change certificate provisioning behavior from the vSphere Web Client.

VMware Certificate Authority mode (default)
When you renew certificates from the vSphere Web Client, VMCA issues the certificates for the hosts. If you changed the VMCA root certificate to include a certificate chain, the host certificates include the full chain.

Custom Certificate Authority mode
Allows you to manually update and use certificates that are not signed or issued by VMCA.

Thumbprint mode
Can be used to retain 5.5 certificates during refresh. Use this mode only temporarily in debugging situations.

Enhanced Linked Mode Overview

Enhanced Linked Mode connects multiple vCenter Server systems together by using one or more Platform Services Controllers.

Enhanced Linked Mode lets you view and search across all linked vCenter Server systems and replicate roles, permissions, licenses, policies, and tags.

When you install vCenter Server or deploy the vCenter Server Appliance with an external Platform Services Controller, you must first install the Platform Services Controller. During installation of the Platform Services Controller, you can select whether to create a new vCenter Single Sign-On domain or join an existing domain. You can select to join an existing vCenter Single Sign-On domain if you have already installed or deployed a Platform Services Controller, and have created a vCenter Single Sign-On domain. When you join an existing vCenter Single Sign-On domain, the data between the existing Platform Services Controller and the new Platform Services Controller is replicated, and the infrastructure data is replicated between the two Platform Services Controllers.

With Enhanced Linked Mode, you can connect not only vCenter Server systems running on Windows but also many vCenter Server Appliances. You can also have an environment where multiple vCenter Server systems and vCenter Server Appliances are linked together.

If you install vCenter Server with an external Platform Services Controller, you first must deploy the Platform Services Controller on one virtual machines or physical server and then deploy vCenter Server on another virtual machines or physical server. While installing vCenter Server, you must select the external Platform Services Controller. Make sure that the Platform Services Controller you select is an external standalone Platform Services Controller. Selecting an existing Platform Services Controller that is a part of an embedded installation is not supported and cannot be reconfigured after the deployment. For information about the recommended topologies, see List of recommended topologies for vSphere 6.0.x.

System Requirements 2

Systems running vCenter Server on Windows, the vCenter Server Appliance, 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 82.

This chapter includes the following topics:

ESXi Requirements

To install ESXi 6.0 or upgrade to ESXi 6.0, your system must meet specific hardware and software requirements.

ESXi Hardware Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi 6.0.

Hardware and System Resources

To install or upgrade ESXi 6.0, 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 6.0 requires a host machine with at least two CPU cores.
- ESXi 6.0 supports 64-bit x86 processors released after September 2006. This includes a broad range of multi-core processors. For a complete list of supported processors, see the VMware compatibility guide at http://www.vmware.com/resources/compatibility.

- ESXi 6.0 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi requires a minimum of 4GB of physical RAM. It is recommended to provide at least 8 GB of RAM to 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 faster Ethernet controllers. For a list of supported network adapter models, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- 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 6.0 host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

For a list of supported storage systems, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility. For Software Fibre Channel over Ethernet (FCoE), see "Installing and Booting ESXi with Software FCoE," on page 53.

ESXi Booting Requirements

vSphere 6.0 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 6.0 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 6.0.

Storage Requirements for ESXi 6.0 Installation or Upgrade

Installing ESXi 6.0 or upgrading to ESXi 6.0 requires a boot device that is a minimum of 1GB in size. When booting from a local disk, SAN or 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 attempts to allocate a scratch region on a separate local disk. If a local disk cannot be found the scratch partition, `/scratch`, is 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, do not leave `/scratch` on the ESXi host ramdisk.

To reconfigure `/scratch`, see "Set the Scratch Partition from the vSphere Web Client," on page 174.

Due to the I/O sensitivity of USB and SD devices the installer does not create a scratch partition on these devices. When installing or upgrading 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. After the installation or upgrade, you should reconfigure `/scratch` to use a persistent datastore. Although a 1GB USB or SD device suffices for a minimal installation, you should use a 4GB or larger device. The extra space will be used for an expanded coredump partition on the USB/SD device. Use a high quality USB flash drive of 16GB or larger so that the extra flash cells can prolong the life of the boot media, but high quality drives of 4GB or larger are sufficient to hold the extended coredump partition. See Knowledge Base article 2004784.

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, you need not 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.

Supported Remote Management Server Models and Firmware Versions

You can use remote management applications to install or upgrade ESXi, or to manage hosts remotely.

Table 2-1. Supported Remote Management Server Models and Minimum Firmware Versions

Remote Management Server Model	Firmware Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
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
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
IBM RSA 2	1.03, 1.2	1.6.0_22

Recommendations for Enhanced ESXi Performance

To enhance performance, install or upgrade 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 23. See also the technical papers on vSphere 5 performance at http://www.vmware.com/resources/techresources/cat/91,203,96.

Table 2-2. Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host. Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3GB of RAM for baseline performance. This figure includes approximately 1024MB for the virtual machines, 256MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines. These calculations do not take into account possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management*.
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS5 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Web Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. **NOTE** For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Web Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 6.0 drivers. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Incoming and Outgoing Firewall Ports for ESXi Hosts

The vSphere Web Client allows you to open and close firewall ports for each service or to allow traffic from selected IP addresses.

The following table lists the firewalls for services that are usually installed. If you install other VIBs on your host, additional services and firewall ports might become available.

Table 2-3. Incoming Firewall Connections

Service	Port	Comment
CIM Server	5988 (TCP)	Server for CIM (Common Information Model).
CIM Secure Server	5989 (TCP)	Secure server for CIM.
CIM SLP	427 (TCP, UDP)	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
DHCPv6	546 (TCP, UDP)	DHCP client for IPv6.
DVSSync	8301, 8302 (UDP)	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.
NFC	902 (TCP)	Network File Copy (NFC) provides a file-type-aware FTP service for vSphere components. ESXi uses NFC for operations such as copying and moving data between datastores by default.
Virtual SAN Clustering Service	12345, 23451 (UDP)	Virtual SAN Cluster Monitoring and Membership Directory Service. Uses UDP-based IP multicast to establish cluster members and distribute Virtual SAN metadata to all cluster members. If disabled, Virtual SAN does not work.
DHCP Client	68 (UDP)	DHCP client for IPv4.
DNS Client	53 (UDP)	DNS client.
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Traffic between hosts for vSphere Fault Tolerance (FT).
NSX Distributed Logical Router Service	6999 (UDP)	NSX Virtual Distributed Router service. The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open. This service was called NSX Distributed Logical Router in earlier versions of the product.
Virtual SAN Transport	2233 (TCP)	Virtual SAN reliable datagram transport. Uses TCP and is used for Virtual SAN storage IO. If disabled, Virtual SAN does not work.
SNMP Server	161 (UDP)	Allows the host to connect to an SNMP server.
SSH Server	22 (TCP)	Required for SSH access.
vMotion	8000 (TCP)	Required for virtual machine migration with vMotion.
vSphere Web Client	902, 443 (TCP)	Client connections
vsanvp	8080 (TCP)	VSAN VASA Vendor Provider. Used by the Storage Management Service (SMS) that is part of vCenter to access information about Virtual SAN storage profiles, capabilities, and compliance. If disabled, Virtual SAN Storage Profile Based Management (SPBM) does not work.
vSphere Web Access	80 (TCP)	Welcome page, with download links for different interfaces.

Table 2-4. Outgoing Firewall Connections

Service	Port	Comment
CIM SLP	427 (TCP, UDP)	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
DHCPv6	547 (TCP, UDP)	DHCP client for IPv6.
DVSSync	8301, 8302 (UDP)	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.
HBR	44046, 31031 (TCP)	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.
NFC	902 (TCP)	Network File Copy (NFC) provides a file-type-aware FTP service for vSphere components. ESXi uses NFC for operations such as copying and moving data between datastores by default.
VVOL	9 (UDP)	Used by the Virtual Volumes feature.
Virtual SAN Clustering Service	12345 23451 (UDP)	Cluster Monitoring, Membership, and Directory Service used by Virtual SAN.
DHCP Client	68 (UDP)	DHCP client.
DNS Client	53 (TCP, UDP)	DNS client.
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Supports VMware Fault Tolerance.
Software iSCSI Client	3260 (TCP)	Supports software iSCSI.
NSX Distributed Logical Router Service	6999 (UDP)	The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open.
rabbitmqproxy	5671 (TCP)	A proxy running on the ESXi host that allows applications running inside virtual machines to communicate to the AMQP brokers running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. The proxy connects to the brokers in the vCenter network domain. Therefore, the outgoing connection IP addresses should at least include the current brokers in use or future brokers. Brokers can be added if customer would like to scale up.
Virtual SAN Transport	2233 (TCP)	Used for RDT traffic (Unicast peer to peer communication) between Virtual SAN nodes.
vMotion	8000 (TCP)	Required for virtual machine migration with vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server agent.
vsanvp	8080 (TCP)	Used for Virtual SAN Vendor Provider traffic.

vCenter Server for Windows Requirements

To install vCenter Server on a Windows virtual machine or physical server, your system must meet specific hardware and software requirements.

- Synchronize the clocks of the virtual machines on which you plan to install vCenter Server and the Platform Services Controller. See "Synchronizing Clocks on the vSphere Network," on page 209.
- Verify that the DNS name of the virtual machine or physical server matches the actual full computer name.
- Verify that the host name of the virtual machine or physical server that you are installing or upgrading vCenter Server on complies with RFC 1123 guidelines.
- Verify that the system on which you are installing vCenter Server is not an Active Directory domain controller.
- If your vCenter Server service is running in a user account other than the Local System account, verify that the user account in which the vCenter Server service is running has the following permissions:
  - **Member of the Administrators group**
  - **Log on as a service**
  - **Act as part of the operating system (if the user is a domain user)**
- 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. Your host machine must be connected to a domain if you want to add Active Directory identity sources after the installation.
- Verify that the LOCAL SERVICE account has read permission on the folder in which vCenter Server is installed and on the HKLM registry.
- Verify that the connection between the virtual machine or physical server and the domain controller is working.

vCenter Server for Windows Pre-Install Checks

When you install vCenter Server and the Platform Services Controller, the installer does a pre-install check, for example, to verify that enough space is available on the virtual machine or physical server where you are installing vCenter Server, and verifies that the external database, if any, can be successfully accessed.

When you deploy vCenter Server with an embedded Platform Services Controller, or an external Platform Services Controller, vCenter Single Sign-On is installed as part of the Platform Services Controller. At the time of installation, the installer provides you with the option to join an existing vCenter Single Sign-On server domain. When you provide the information about the other vCenter Single Sign-On service, the installer uses the administrator account to check the host name and password, to verify that the details of the vCenter Single Sign-On server you provided can be authenticated before proceeding with the installation process.

The pre-install checker performs checks for the following aspects of the environment:

- Windows version
- Minimum processor requirements
- Minimum memory requirements
- Minimum disk space requirements
- Permissions on the selected install and data directory

- Internal and external port availability
- External database version
- External database connectivity
- Administrator privileges on the Windows machine
- Any credentials that you enter

For information about the minimum storage requirements, see "vCenter Server for Windows Storage Requirements," on page 30. For information about the minimum hardware requirements, see "vCenter Server for Windows Hardware Requirements," on page 30.

vCenter Server for Windows Hardware Requirements

When you install vCenter Server on a virtual machine or physical server running Microsoft Windows, your system must meet specific hardware requirements.

You can install vCenter Server and the Platform Services Controller on the same virtual machine or physical server or on different virtual machines or physical servers. When you install vCenter Server with an embedded Platform Services Controller, you install vCenter Server and the Platform Services Controller on the same virtual machine or physical server. When you install the vCenter Server with an external Platform Services Controller, first install the Platform Services Controller that contains all of the required services on one virtual machine or physical server, and then install vCenter Server and the vCenter Server components on another virtual machine or physical server.

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

Table 2-5. Minimum Recommended Hardware Requirements for Installing vCenter Server on a Windows Machine

	Platform Services Controller	Tiny Environment (up to 10 Hosts, 100 Virtual Machines)	Small Environment (up to 100 Hosts, 1000 Virtual Machines)	Medium Environment (up to 400 Hosts, 4,000 Virtual Machines)	Large Environment (up to 1,000 Hosts, 10,000 Virtual Machines)
Number of CPUs	2	2	4	8	16
Memory	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

Important For vCenter Server with an embedded Platform Services Controller, you must add the hardware requirements for Platform Services Controller to the hardware requirements for vCenter Server depending on the size of your environment.

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

vCenter Server for Windows Storage Requirements

When you install vCenter Server, your system must meet minimum storage requirements.

The storage requirements per folder depend on the deployment model that you decide to install. During installation, you can select a folder other than the default `C:\Program Files\VMware` folder to install vCenter Server and the Platform Services Controller. You can also select a folder other than the default `C:\ProgramData\VMware\vCenterServer\` in which to store data.

Table 2-6. vCenter Server Minimum Storage Requirements Depending On the Deployment Model

Default Folder	vCenter Server with an Embedded Platform Services Controller	vCenter Server with an External Platform Services Controller	External Platform Services Controller
`Program Files`	6 GB	6 GB	1 GB
`ProgramData`	8 GB	8 GB	2 GB
System folder (to cache the MSI installer)	3 GB	3 GB	1 GB

vCenter Server for Windows 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 the external database.

The earliest Windows Server version that vCenter Server supports is Windows Server 2008 SP2. Your Windows Server must have the latest updates and patches installed. For a full list of supported operating systems, see Supported host Operating Systems for VMware vCenter Server installation.

vCenter Server for Windows Database Requirements

vCenter Server requires a database to store and organize server data.

Each vCenter Server instance must have its own database. For environments with up to 20 hosts and 200 virtual machines, you can use the bundled PostgreSQL database that the vCenter Server installer can install and set up for you during the vCenter Server installation. Larger installations require a supported database.

During vCenter Server installation or upgrade, you must select to install the embedded database or point the vCenter Server system to any existing supported database. vCenter Server 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.

vCenter Server Appliance Requirements

You can deploy the vCenter Server Appliance on a host running ESXi 5.0 or later. Your system must also meet specific software and hardware requirements.

When you use Fully Qualified Domain Names, make sure that the machine you use for deploying the vCenter Server Appliance and the ESXi host are on the same DNS server.

Before you deploy the vCenter Server Appliance, synchronize the clocks of all virtual machines on the vSphere network. Unsynchronized clocks might result in authentication problems and can cause the installation to fail or prevent the vCenter Server services from starting. See "Synchronizing Clocks on the vSphere Network," on page 209.

vCenter Server Appliance Hardware Requirements

When you deploy the vCenter Server Appliance, you can select to deploy an appliance that is suitable for the size of your vSphere environment. The option that you select determine the number of CPUs and the amount of memory that the appliance will have.

The hardware requirements such as number of CPUs and memory depend on the size of your vSphere inventory.

Table 2-7. Hardware Requirements for VMware vCenter Server Appliance

Resources	Platform Services Controller	Tiny Environment (up to 10 Hosts, 100 Virtual Machines)	Small Environment (up to 100 Hosts, 1,000 Virtual Machines)	Medium Environment (up to 400 Hosts, 4,000 Virtual Machines)	Large Environment (up to 1,000 Hosts, 10,000 Virtual Machines)
Number of CPUs	2	2	4	8	16
Memory	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

IMPORTANT For vCenter Server Appliance with an embedded Platform Services Controller, you must add the hardware requirements for Platform Services Controller to the hardware requirements for vCenter Server Appliance depending on the size of your environment.

vCenter Server Appliance Storage Requirements

When you deploy the vCenter Server Appliance, the host on which you deploy the appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment, but also on the disk provisioning mode.

The storage requirements depend on the deployment model that you select to deploy.

Table 2-8. vCenter Server Minimum Storage Requirements Depending On the Deployment Model

	vCenter Server Appliance with an Embedded Platform Services Controller	vCenter Server Appliance with an External Platform Services Controller	External Platform Services Controller Appliance
Tiny environment (up to 10 hosts, 100 virtual machines)	120 GB	86 GB	30 GB
Small environment (up to 100 hosts, 1,000 virtual machines)	150 GB	108 GB	30 GB
Medium environment (up to 400 hosts, 4,000 virtual machine)	300 GB	220 GB	30 GB
Large environment (up to 1,000 hosts, 10,000 virtual machines)	450 GB	280 GB	30 GB

Software Included in the 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 package contains the following software:

- SUSE Linux Enterprise Server 11 Update 3 for VMware, 64-bit edition
- PostgreSQL
- vCenter Server 6.0 and vCenter Server 6.0 components.

vCenter Server Appliance Software Requirements

The VMware vCenter Server Appliance can be deployed only on hosts that are running ESXi version 5.0 or later.

You can deploy the vCenter Server Appliance only by using the Client Integration Plug-In, which is an HTML installer for Windows that you can use to connect directly to an ESXi 5.0.x, ESXi 5.1.x, ESXi 5.5.x, or ESXi 6.0 host and deploy the vCenter Server Appliance on the host.

IMPORTANT You cannot deploy the vCenter Server Appliance by using the vSphere Client or the vSphere Web Client. During the deployment of the vCenter Server Appliance you must provide various inputs, such as Operating System and vCenter Single Sign-On passwords. If you try to deploy the appliance by using the vSphere Client or the vSphere Web Client, you are not prompted to provide such inputs and the deployment fails.

vCenter Server Appliance Database Requirements

The vCenter Server Appliance requires a database to store and organize server data.

Each vCenter Server Appliance instance must have its own database. You can use the bundled PostgreSQL database that is included in the vCenter Server Appliance, which supports up to 1,000 hosts and 10,000 virtual machines.

For external databases, the vCenter Server Appliance supports only Oracle databases. These Oracle databases are of the same versions shown in the VMware Product Interoperability Matrix for the version of the vCenter Server that you are installing. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

If you want to use an external database, make sure that you create a 64-bit DSN so that vCenter Server can connect to the Oracle database.

vCenter Server Required Ports

The vCenter Server system both on Windows and in the appliance, must be able to send data to every managed host and receive data from the vSphere Web Client and the Platform Services Controller services. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other.

If a port is in use or is blacklisted, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation. There are internal ports that are used only for inter-process communication.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a firewall exists between any of these elements, the installer opens the ports during the installation or upgrade process. 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 and later, firewall is enabled by default.

Table 2-9. Ports Required for Communication Between Components

Port	Description	Can Be Changed During Installation
22	System port for SSHD. This port is used only by the vCenter Server Appliance.	No
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server. WS-Management (also requires port 443 to be open). If you use a Microsoft SQL database that is stored on the same virtual machine or physical server as the vCenter Server, port 80 is used by the SQL Reporting Service. When you install or upgrade vCenter Server, the installer prompts you to change the HTTP port for vCenter Server. Change the vCenter Server HTTP port to a custom value to ensure a successful installation or upgrade.	Yes
88	VMware key distribution center port.	No
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. 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.	No
443	The default port that the vCenter Server system uses to listen for connections from the vSphere Web Client. To enable the vCenter Server system to receive data from the vSphere Web Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. This port is also used for the following services: ■ WS-Management (also requires port 80 to be open) ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts	Yes
514	vSphere Syslog Collector port for vCenter Server on Windows and vSphere Syslog Service port for vCenter Server Appliance	Yes
636	For vCenter Server Enhanced 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.	No
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	Yes
1514	vSphere Syslog Collector TLS port for vCenter Server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance	Yes
2012	Control interface RPC for vCenter Single Sign-On	No
2014	RPC port for all VMCA (VMware Certificate Authority) APIs	Yes

Table 2-9. Ports Required for Communication Between Components (Continued)

Port	Description	Can Be Changed During Installation
2020	Authentication framework management	Yes
6500	ESXi Dump Collector port	Yes
6501	Auto Deploy service	Yes
6502	Auto Deploy management	Yes
7444	Secure Token Service	No
9443	vSphere Web Client HTTPS	No
11711	vCenter Single Sign-On LDAP	No
11712	vCenter Single Sign-On LDAPS	No

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

For more information about firewall configuration, see the *vSphere Security* documentation.

vSphere DNS Requirements

You install or upgrade vCenter Server, like any other network server, on a host 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. When you install vCenter Server and the Platform Services Controller, you must provide the fully qualified domain name (FQDN) or the static IP of the host machine on which you are performing the install or upgrade. The recommendation is to use the FQDN.

When you deploy the vCenter Server Appliance, you can assign a static IP to the appliance. This way, you ensure that in case of system restart, the IP address of the vCenter Server Appliance remains the same.

Ensure that DNS reverse lookup returns an FQDN when queried with the IP address of the host machine on which vCenter Server is installed. When you install or upgrade vCenter Server, the installation or upgrade of the Web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server host machine from its IP address. Reverse lookup is implemented using PTR records.

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

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Web Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Web Clients.

Verify That the FQDN is Resolvable

You install or upgrade vCenter Server, like any other network server, on a virtual machine or physical server with a fixed IP address and well-known DNS name, so that clients can reliably access the service.

If you plan to use a FQDN, for the virtual machine or physical server on which you install or upgrade vCenter Server, you must verify that the FQDN is resolvable.

Procedure

- ◆ At the Windows command prompt, run the `nslookup` command.

```
nslookup -nosearch -nodefname your_vCenter_Server_FQDN
```

If the FQDN is resolvable, the `nslookup` command returns the IP address and name of the vCenter Server virtual machine or physical server.

vSphere Web Client Software Requirements

Make sure that your browser supports the vSphere Web Client.

The vSphere Web Client 6.0 requires Adobe Flash Player 16 or later. The latest Adobe Flash Player version for Linux systems is 11.2. Therefore, the vSphere Web Client cannot run on Linux platforms.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Web Client. For best performance, use Google Chrome.

Table 2-10. Supported Guest Operating Systems and Minimum Browser Versions for the vSphere Web Client

Operating system	Browser
Windows	Microsoft Internet Explorer 10.0.19 and later. Mozilla Firefox 34 and later. Google Chrome 39 and later.
Mac OS	Mozilla Firefox 34 and later. Google Chrome 39 and later.

Client Integration Plug-In Software Requirements

If you plan to install the Client Integration Plug-in separately from the vSphere Web Client so that you can connect to an ESXi host and deploy or upgrade the vCenter Server Appliance, make sure that your browser supports the Client Integration Plug-in.

To use the Client Integration Plug-in, verify that you have one of the supported Web browsers.

Table 2-11. Supported Web Browsers

Browser	Supported Versions
Microsoft Internet Explorer	Version 10 and 11
Mozilla Firefox	Version 30 and later
Google Chrome	Version 35 and later

vSphere Client Requirements

You can install the vSphere Client to manage single ESXi host. The Windows system on which you install the vSphere Client must meet specific hardware and software requirements.

vSphere Client Hardware Requirements

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

vSphere Client Minimum Hardware Requirements and Recommendations

Table 2-12. vSphere Client Minimum Hardware Requirements and Recommendations

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

vSphere Client 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, see Supported host operating systems for vSphere Client (Windows) installation.

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.

TCP and UDP Ports for the vSphere Client

ESXi hosts and other network components are accessed using predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports.

The table lists TCP and UDP ports, and the purpose and the type of each. Ports that are open by default at installation time are indicated by (Default).

Table 2-13. TCP and UDP Ports

Port	Purpose	Traffic Type
443 (Default)	HTTPS access vSphere Client access to vCenter Server vSphere Client access to ESXi hosts vSphere Client access to vSphere Update Manager	Incoming TCP
902 (Default)	vSphere Client access to virtual machine consoles	Incoming and outgoing TCP, outgoing UDP
903	Remote console traffic generated by user access to virtual machines on a specific host. vSphere Client access to virtual machine consoles MKS transactions (xinetd/vmware-authd-mks)	Incoming TCP

Required Free Space for System Logging

If you used Auto Deploy to install your ESXi 6.0 host, 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 is available for system logging .

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.

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

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 6.0 configures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 2-14. 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)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

For information about setting up a remote log server, see "Configure Syslog on ESXi Hosts," on page 176.

Before You Install ESXi 3

Before you install ESXi, understand the installation process and options.

This chapter includes the following topics:

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 "Installing ESXi Interactively," on page 55.

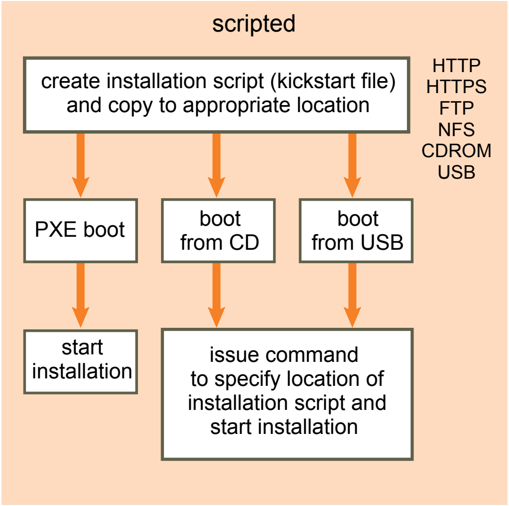
Scripted ESXi Installation

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 "Installing or Upgrading Hosts by Using a Script," on page 58.

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 3-1. Scripted Installation


scripted
create installation script (kickstart file) and copy to appropriate location
HTTP
HTTPS
FTP
NFS
CDROM
USB
PXE boot
boot from CD
boot from USB
start installation
issue command to specify location of installation script and start installation

Auto Deploy ESXi Installation

vSphere 5.x and vSphere 6.0 provide several ways to install ESXi with Auto Deploy.

These topics describe Auto Deploy options for ESXi installation.

Provisioning ESXi Hosts by Using vSphere Auto Deploy

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

When you provision hosts by using Auto Deploy, vCenter Server loads the ESXi image directly into the host memory. Auto Deploy does not store the ESXi state on the host disk.

vCenter Server makes ESXi updates and patches available for download in the form of an image profile. Optionally, the host configuration is provided in the form of a host profile. You can create host profiles by using the vSphere Web Client. You can create custom image profiles by using ESXi Image Builder CLI. See "Using vSphere ESXi Image Builder," on page 137 and *vSphere Host Profiles*.

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

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

See "Understanding vSphere Auto Deploy," on page 72.

Using vSphere Auto Deploy for Stateful Installations

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

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

See "Using Auto Deploy for Stateless Caching and Stateful Installs," on page 94.

vSphere Auto Deploy and Stateless Caching

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

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

See "Using Auto Deploy for Stateless Caching and Stateful Installs," on page 94.

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 "Using vSphere ESXi Image Builder," on page 137 and "Installing ESXi Using vSphere Auto Deploy," on page 71.

About ESXi Evaluation and Licensed Modes

You can use evaluation mode to explore the entire set of features for ESXi hosts. The evaluation mode provides the set of features equal to a vSphere Enterprise Plus license. Before the evaluation mode expires, you must assign to your hosts a license that supports all the features in use.

For example, in evaluation mode, you can use vSphere vMotion technology, the vSphere HA feature, the vSphere DRS feature, and other features. If you want to continue using these features, you must assign a license that supports them.

The installable version of ESXi hosts is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal storage 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. At any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. The time available in the evaluation period is decreased by the time already used.

For example, suppose that you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard Edition license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features for the host for the remaining evaluation period of 40 days.

For information about managing licensing for ESXi hosts, see the *vCenter Server and Host Management* documentation.

Media Options for Booting the ESXi Installer

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

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 42.
- Boot from a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 42.
- PXE boot from the network. "PXE Booting the ESXi Installer," on page 46
- Boot from a remote location using a remote management application. See "Using Remote Management Applications," on page 53

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 45.

Procedure

1 Download the ESXi installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

  ESXi is listed under Datacenter & Cloud Infrastructure.

2 Confirm that the md5sum is correct.

  See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

3 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.

Perform the procedure on a Linux machine with an operating system that can detect the USB flash drive. In the examples, the operating system detects the USB flash drive as `/dev/`*`sdb`*.

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

Prerequisites

- The ESXi ISO image `VMware-VMvisor-Installer-`*`6.x.x-XXXXXX`*`.x86_64.iso`, including the `isolinux.cfg` file, where *`6.x.x`* is the version of ESXi that you are installing, and *`XXXXXX`* is the build number of the installer ISO image
- Linux machine with access to Syslinux version 3.86 or 4.03

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 At the command line, run the following command.

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

   This command displays the current log messages.

   b Plug in your USB flash drive.

   You see several messages that identify 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, in place of *sdb*.

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 a 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 exit the program.

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-version_directory/syslinux-version/bin/syslinux /dev/sdb1
   cat /path_to_syslinux-version_directory/syslinux-version/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-6.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 `/usbdisk/syslinux.cfg` file, change the `APPEND -c boot.cfg` line to `APPEND -c boot.cfg -p 1`.

10 If you use Syslinux version 4.03, replace `menu.c32`.

```
cp / path_to_syslinux directory/syslinux-4.03/usr/share/syslinux/menu.c32 /usbdisk/
```

11 Unmount the USB flash drive.

```
umount /usbdisk
```

12 Unmount the installer ISO image.

```
umount /esxi_cdrom
```

The USB flash drive can 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 58 and "About PXE Configuration Files," on page 49.

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 customization 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 60 and "About the boot.cfg File," on page 68.

Prerequisites

- Linux machine
- The ESXi ISO image `VMware-VMvisor-Installer-`*`6.x.x-XXXXXX`*`.x86_64.iso`,where *`6.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 in a folder:

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount
```

`XXXXXX` is the ESXi build number for the version that you are installing or upgrading to.

3 Copy the contents of `cdrom` to another folder:

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

4 Copy the kickstart file to `/esxi_cdrom`.

```
cp ks_cust.cfg /esxi_cdrom
```

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

This step automates the installation or upgrade, 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 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 start the ESXi installer from a network interface.

ESXi 6.0 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 by using PXE.

PXE uses Dynamic Host Configuration Protocol (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 can run ESXi have network adapters that can PXE boot.

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

About the TFTP Server, PXELINUX, and gPXE

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

Most Linux distributions include a copy of the tftp-hpa server. If you require a supported solution, purchase a supported TFTP server from your vendor of choice.

If your TFTP server will run on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/. Earlier versions of tftpd32 were incompatible with PXELINUX and gPXE.

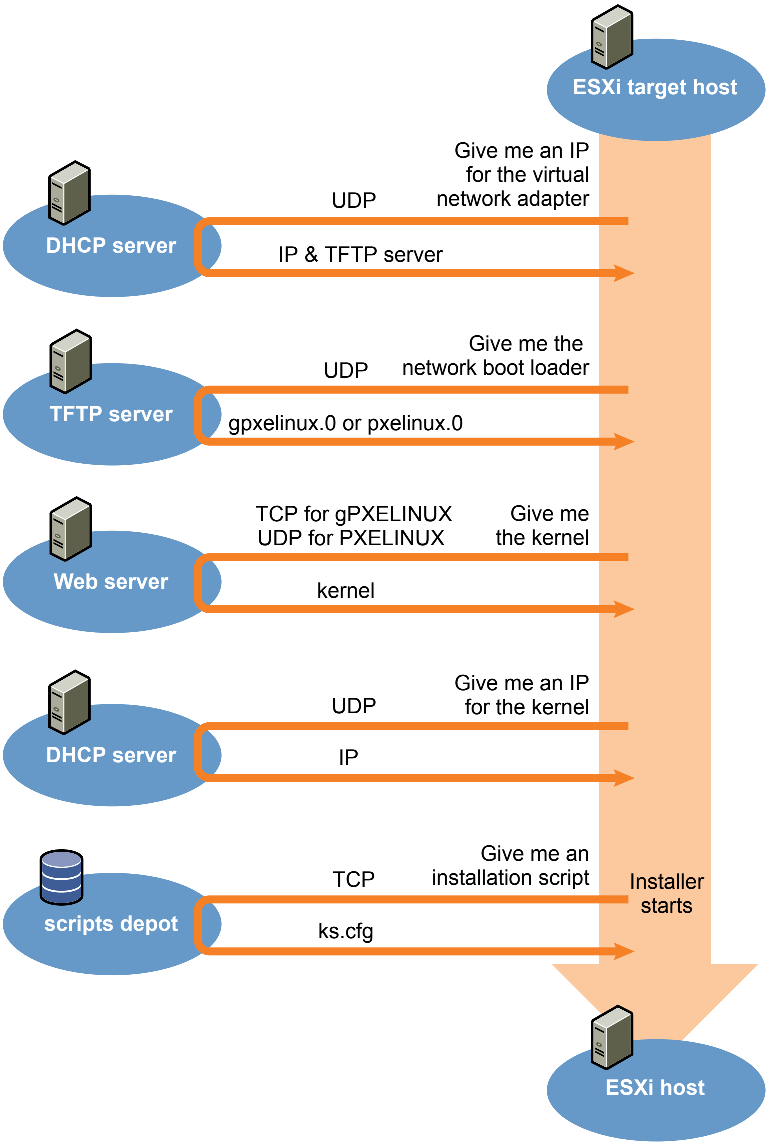
You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.

The PXELINUX and gPXE environments allow your target machine to boot the ESXi installer. PXELINUX is part of the SYSLINUX package, which can be found at http://www.kernel.org/pub/linux/utils/boot/syslinux/, although many Linux distributions include it. Many versions of PXELINUX also include gPXE. Some distributions, such as Red Hat Enterprise Linux version 5.3, include earlier versions of PXELINUX that do not include gPXE.

If you do not use gPXE, you might experience problems while booting the ESXi installer on a heavily loaded network TFTP is sometimes unreliable for transferring large amounts of data. If you use PXELINUX without gPXE, the `pxelinux.0` binary file, the configuration file, the kernel, and other files are transferred by TFTP. If you use gPXE, only the `gpxelinux.0` binary file and configuration file are transferred by TFTP. With gPXE, you can use a Web server to transfer the kernel and other files required to boot the ESXi installer.

NOTE VMware tests PXE booting with PXELINUX version 3.86. This is not a statement of limited support. For support of third-party agents that you use to set up your PXE booting infrastructure, contact the vendor.

Figure 3-2. Overview of PXE Boot Installation Process



Sample DHCP Configuration

To PXE boot the ESXi installer, the DHCP server must send the address of the TFTP server and a pointer to the `pxelinux.0` or `gpxelinux.0` directory.

The DHCP server is used by the target machine to obtain an IP address. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the PXELINUX binary (which usually resides on a TFTP server). When the target machine first boots, it broadcasts a packet across the network requesting this information to boot itself. The DHCP server responds.

⚠ CAUTION Do not set up a new DHCP server if your network already has one. If multiple DHCP servers respond to DHCP requests, machines can obtain incorrect or conflicting IP addresses, or can fail to receive the proper boot information. Talk to a network administrator before setting up a DHCP server. For support on configuring DHCP, contact your DHCP server vendor.

Many DHCP servers can PXE boot hosts. If you are using a version of DHCP for Microsoft Windows, see the DHCP server documentation to determine how to pass the `next-server` and `filename` arguments to the target machine.

gPXE Example

This example shows how to configure a ISC DHCP version 3.0 server to enable gPXE.

```
allow booting;
allow bootp;
# gPXE options
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.bus-id code 177 = string;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server TFTP server address;
   if not exists gpxe.bus-id {
      filename "/gpxelinux.0";
   }
}
subnet Network address netmask Subnet Mask {
   range Starting IP Address Ending IP Address;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `gpxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

PXELINUX (without gPXE) Example

This example shows how to configure a ISC DHCP version 3.0 server to enable PXELINUX.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xx.xx;
   filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
   range 192.168.48.100 192.168.48.250;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

About PXE Configuration Files

The PXE configuration file defines the menu displayed to the target ESXi host as it boots up and contacts the TFTP server. You need a PXE configuration file to PXE boot the ESXi installer.

The TFTP server constantly listens for PXE clients on the network. When it detects that a PXE client is requesting PXE services, it sends the client a network package that contains a boot menu.

Required Files

In the PXE configuration file, you must include paths to the following files:

- `mboot.c32` is the boot loader.
- `boot.cfg` is the boot loader configuration file.

See "About the boot.cfg File," on page 68

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 60 and "About the boot.cfg File," on page 68.

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 46.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 47.
- PXELINUX.
- Server with a hardware configuration that is supported with your version of ESXi. See VMware 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 60.

- 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. To specify the VLAN ID to be used with PXE booting, verify 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, `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 to the line after 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 that contains 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-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Name the file with the media access control (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 by using PXELINUX, and you can use the isolinux.cfg file as the PXE configuration file.

See also "About Installation and Upgrade Scripts," on page 60 and "About the boot.cfg File," on page 68

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 46.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 47.
- PXELINUX.
- Server with a hardware configuration that is supported with your version of ESXi. See the VMware Compatibility Guide 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 60.
- 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. To specify the VLAN ID to be used with PXE booting, verify 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.

   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, `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 after the `kernel` command to specify the location of the installation script.

   In the following example, *XXX.XXX.XXX.XXX* is the IP address of the server where the installation script resides.

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

6 Copy the `isolinux.cfg` file from the ESXi installer ISO image to the `/tftpboot/pxelinux.cfg` directory.

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

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

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

8 Boot the machine with the network adapter.

PXE Boot the ESXi Installer Using gPXE

You can PXE boot the ESXi installer using gPXE.

See also "About Installation and Upgrade Scripts," on page 60 and "About the boot.cfg File," on page 68

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 47.
- Server with a hardware configuration that is supported with your version of ESXi. 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 60.

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.t00 ---
   http://XXX.XXX.XXX.XXX/tools.t00 --- http://XXX.XXX.XXX.XXX/imgdb.tgz ---
   http://XXX.XXX.XXX.XXX/imgpayld.tgz
   ```

3. gPXE boot the host and press Ctrl+B to access the GPT menu.

4. Enter the following commands to boot with the ESXi installer, where *XXX.XXX.XXX.XXX* is the HTTP server IP address.

   ```
   dhcp net0 ( if dchp is not set)
   kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
   imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
   boot mboot.c32
   ```

Installing and Booting ESXi with Software FCoE

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

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

Using Remote Management Applications

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

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see "Supported Remote Management Server Models and Firmware Versions," on page 25. For support on remote management applications, contact the vendor.

You can use remote management applications to do both interactive and scripted installations of ESXi remotely.

If you use remote management applications to install ESXi, the virtual CD might encounter corruption problems with systems or networks operating at peak capacity. If a remote installation from an ISO image fails, complete the installation from the physical CD media.

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 3-1. Required Information for ESXi Installation

Information	Required or Optional	Default	Comments
Keyboard layout	Required	U.S. English	
VLAN ID	Optional	None	Range: 0 through 4094
IP address	Optional	DHCP	You can allow DHCP to configure the network during installation. After installation, you can change the network settings.
Subnet mask	Optional	Calculated based on the IP address	
Gateway	Optional	Based on the configured IP address and subnet mask	
Primary DNS	Optional	Based on the configured IP address and subnet mask	
Secondary DNS	Optional	None	
Host name	Required for static IP settings	None	The vSphere Web Client can use either the host name or the IP address to access the ESXi host.
Install location	Required	None	Must be at least 5 GB if you install the components on a single disk.
Migrate existing ESXi settings. Preserve existing VMFS datastore.	Required if you are installing ESXi on a drive with an existing ESXi installation.	None	If you have an existing ESXi 5.x installation, the ESXi installer offers a choice between preserving or overwriting the VMFS datastore during installation
Root password	Optional	None	The root password must contain between 8 and 40 characters. For information about passwords see the *vSphere Security* documentation.

Download the ESXi Installer

Download the installer for ESXi.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1 Download the ESXi installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

ESXi is listed under Datacenter & Cloud Infrastructure.

2 Confirm that the md5sum is correct.

See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

Installing ESXi 4

You can install ESXi interactively, with a scripted installation, or with vSphere Auto Deploy.

This chapter includes the following topics:

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.

Install ESXi Interactively

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

Prerequisites

- You must have the ESXi installer ISO in one of the following locations:
  - On CD or DVD. If you do not have the installation CD/DVD, you can create one. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 42
  - On a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 42.

  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 46.

- 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 53.
- 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 53.
- Verify that ESXi Embedded is not present on the host machine. ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1. Insert the ESXi installer CD/DVD into the CD/DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device or the USB flash drive.

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

   Press F1 for information about the selected disk.

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

   If you select a disk that 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.

   If you select a disk that is in Virtual SAN disk group, the resulting installation depends on the type of disk and the group size:

   - If you select an SSD, the SSD and all underlying HDDs in the same disk group will be wiped.
   - If you select an HDD, and the disk group size is greater than two, only the selected HDD will be wiped.
   - If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD will be wiped.

   For more information about managing Virtual SAN disk groups, see the *vSphere Storage* documentation.
4. Select the keyboard type for the host.

   You can change the keyboard type after installation in the direct console.
5. Enter the root password for the host.

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

6 Press Enter to start the installation.

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

8 Press Enter to reboot the host.

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

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

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

   NOTE UEFI systems might require additional steps to set the boot device. See "Host Fails to Boot After You Install ESXi in UEFI Mode," on page 166

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 6, "After You Install and Set Up ESXi," on page 181.

Install ESXi on a Software iSCSI Disk

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

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

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

Prerequisites

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

Procedure

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

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

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

3 Follow the prompts to complete the installation.

4 Reboot the host.

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

See the vendor documentation for your system.

What to do next

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

Installing or Upgrading Hosts by Using a Script

You can quickly deploy ESXi hosts by using scripted, unattended installations or upgrades. Scripted installations or upgrades 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 or upgrade, you must use the supported commands to create a script. You can 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 server
- HTTP/HTTPS server
- NFS server
- USB flash drive
- CD-ROM drive

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 61.

Enter Boot Options to Start an Installation or Upgrade Script

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

At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See "About the boot.cfg File," on page 68 and "PXE Booting the ESXi Installer," on page 46.

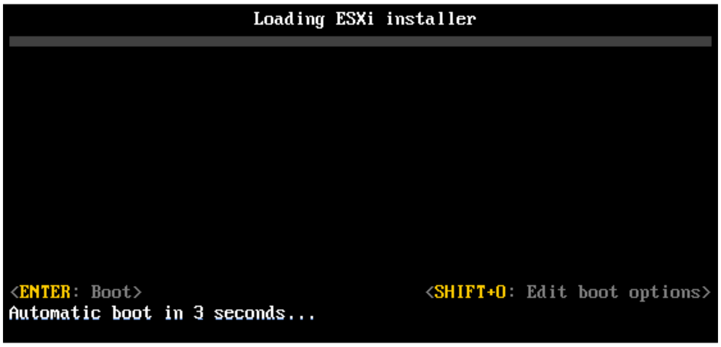
To specify the location of the installation script, set the `ks=`*`filepath`* option, where *filepath* is indicates the location of your Kickstart file. Otherwise, a scripted installation or upgrade cannot start. If `ks=`*`filepath`* is omitted, the text installer is run.

Supported boot options are listed in "Boot Options," on page 59.

Procedure

1 Start the host.

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



```
                    Loading ESXi installer

<ENTER: Boot>                        <SHIFT+O: Edit boot options>
Automatic boot in 3 seconds...
```

3 At the `runweasel` command prompt, type **`ks=`*`location of installation script plus boot command-line options`***.

Example: Boot Option

You type the following boot options:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Boot Options

When you perform a scripted installation, you might need to specify options at boot time to access the kickstart file.

Supported Boot Options

Table 4-2. Boot Options for ESXi Installation

Boot Option	Description
`BOOTIF=`*`hwtype-MAC address`*	Similar to the `netdevice` option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`gateway=`*`ip address`*	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
`ip=`*`ip address`*	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`ks=cdrom:/`*`path`*	Performs a scripted installation with the script at *path*, which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found.

Table 4-2. Boot Options for ESXi Installation (Continued)

Boot Option	Description
`ks=file://`*`path`*	Performs a scripted installation with the script at *path*.
`ks=`*`protocol`*`://`*`serverpath`*	Performs a scripted installation with a script located on the network at the given URL. *protocol* can be `http`, `https`, `ftp`, or `nfs`. An example using nfs protocol is `ks=nfs://`*`host`*`:`*`porturl-path`*. The format of an NFS URL is specified in RFC 2224.
`ks=usb`	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named `ks.cfg`. The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the `ks.cfg` file is found. Only FAT16 and FAT32 file systems are supported.
`ks=usb:/`*`path`*	Performs a scripted installation with the script file at the specified path, which resides on USB.
`ksdevice=`*`device`*	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`nameserver=`*`ip address`*	Specifies a domain name server to be used for downloading the installation script and installation media.
`netdevice=`*`device`*	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`netmask=`*`subnet mask`*	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
`vlanid=`*`vlanid`*	Configure the network card to be on the specified VLAN.

About Installation and Upgrade Scripts

The installation/upgrade script is a text file, for example `ks.cfg`, that contains supported commands.

The command section of the script contains the ESXi installation options. This section is required and must appear first in the script.

About the Default ks.cfg Installation Script

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

The default `ks.cfg` installation script is located in the initial RAM disk at `/etc/vmware/weasel/ks.cfg`. You can specify the location of the default `ks.cfg` file with the `ks=file://etc/vmware/weasel/ks.cfg` boot option. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 58.

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 use the vSphere Web Client to log in to the vCenter Server that manages the ESXi host and 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 45.
- USB Flash drive. See "Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script," on page 44.
- A network location accessible through the following protocols: NFS, HTTP, HTTPS, FTP

Path to the Installation or Upgrade Script

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

`ks=http://`*`XXX.XXX.XXX.XXX`*`/kickstart/KS.CFG` is the path to the ESXi installation script, where *`XXX.XXX.XXX.XXX`* is the IP address of the machine where the script resides. See "About Installation and Upgrade Scripts," on page 60.

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 58.

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.

accepteula or vmaccepteula (required)

Accepts the ESXi license agreement.

clearpart (optional)

Clears any existing partitions on the disk. Requires the `install` command to be specified. Carefully edit the `clearpart` command in your existing scripts.

`--drives=`
Remove partitions on the specified drives.

`--alldrives`
Ignores the `--drives=` requirement and allows clearing of partitions on every drive.

`--ignoredrives=`
Removes partitions on all drives except those specified. Required unless the `--drives=` or `--alldrives` flag is specified.

`--overwritevmfs`
Allows overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.

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

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

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

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

dryrun (optional)

Parses and checks the installation script. Does not perform the installation.

install

Specifies that this is a fresh installation. Replaces the deprecated `autopart` command used for ESXi 4.1 scripted installations. Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

`--disk= or --drive=`
Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 68.

`--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`.

`--ignoressd`

Excludes solid-state disks from eligibility for partitioning. This option can be used with the `install` command and the `--firstdisk` option. This option takes precedence over the `--firstdisk` option. This option is invalid with the `--drive` or `--disk` options and with the `upgrade` and `installorupgrade` commands. See the *vSphere Storage* documentation for more information about preventing SSD formatting during auto-partitioning.

`--overwritevsan`

You must use the `--overwritevsan` option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a Virtual SAN disk group. If you use this option and no Virtual SAN partition is on the selected disk, the installation will fail. When you install ESXi on a disk that is in Virtual SAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group will be wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD will be wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD will be wiped.

For more information about managing Virtual SAN disk groups, see the *vSphere Storage* documentation.

`--overwritevmfs`

Required to overwrite an existing VMFS datastore on the disk before installation.

`--preservevmfs`

Preserves an existing VMFS datastore on the disk during installation.

`--novmfsondisk`

Prevents a VMFS partition from being created on this disk. Must be used with `--overwritevmfs` if a VMFS partition already exists on the disk.

installorupgrade

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

`--disk=` or `--drive=`

Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 68.

`--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`.

`--overwritevsan`

You must use the `--overwritevsan` option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a Virtual SAN disk group. If you use this option and no Virtual SAN partition is on the selected disk, the installation will fail. When you install ESXi on a disk that is in a Virtual SAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group will be wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD will be wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD will be wiped.

For more information about managing Virtual SAN disk groups, see the *vSphere Storage* documentation.

`--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.

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
- Ukrainian
- United Kingdom

serialnum or vmserialnum (optional)

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

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

network (optional)

Specifies a network address for the system.

`--bootproto=[dhcp|static]` Specifies whether to obtain the network settings from DHCP or set them manually.

`--device=` Specifies either the MAC address of the network card or the device name, in the form `vmnicNN`, as in `vmnic0`. This options refers to the uplink device for the virtual switch.

--ip=

Sets an IP address for the machine to be installed, in the form xxx.xxx.xxx.xxx. Required with the --bootproto=static option and ignored otherwise.

--gateway=

Designates the default gateway as an IP address, in the form xxx.xxx.xxx.xxx. Used with the --bootproto=static option.

--nameserver=

Designates the primary name server as an IP address. Used with the --bootproto=static option. Omit this option if you do not intend to use DNS.

The --nameserver option can accept two IP addresses. For example: --nameserver="10.126.87.104[,10.126.87.120]"

--netmask=

Specifies the subnet mask for the installed system, in the form 255.xxx.xxx.xxx. Used with the --bootproto=static option.

--hostname=

Specifies the host name for the installed system.

--vlanid= ***vlanid***

Specifies which VLAN the system is on. Used with either the --bootproto=dhcp or --bootproto=static option. Set to an integer from 1 to 4096.

--addvmportgroup=(0|1)

Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (optional)

Causes warning messages to interrupt the installation. If you omit this command, warning messages are logged.

part or partition (optional)

Creates an additional VMFS datastore on the system. Only one datastore per disk can be created. Cannot be used on the same disk as the install command. Only one partition can be specified per disk and it can only be a VMFS partition.

datastore name

Specifies where the partition is to be mounted.

--ondisk= or --ondrive=

Specifies the disk or drive where the partition is created.

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

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

1 Locally attached storage (local)

2 Network storage (remote)

3 USB disks (usb)

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

reboot (optional)

Reboots the machine after the scripted installation is complete.

`<--noeject>` The CD is not ejected after the installation.

rootpw (required)

Sets the root password for the system.

`--iscrypted` Specifies that the password is encrypted.

`password` Specifies the password value.

upgrade

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

`--disk= or --drive=` Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID:`--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 68.

`--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`.

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

--timeout=secs
Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully terminated.

--ignorefailure =[true|false]
If true, the installation is considered a success even if the `%post` script terminated with an error.

%firstboot

Creates an `init` script that runs only during the first boot. The script has no effect on subsequent boots. If multiple `%firstboot` sections are specified, they run in the order that they appear in the kickstart file.

NOTE You cannot check the semantics of `%firstboot` scripts until the system is booting for the first time. A `%firstboot` script might contain potentially catastrophic errors that are not exposed until after the installation is complete.

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

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

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	Example	Description
VML	vml.00025261	The device name as reported by the VMkernel
MPX	mpx.vmhba0:C0:T0:L0	The device name

About the boot.cfg File

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

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

The `boot.cfg` file has the following syntax:

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

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

# Any other line must remain unchanged.
```

The commands in `boot.cfg` configure the boot loader.

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

Command	Description
`title=`*`STRING`*	Sets the boot loader title to *`STRING`*.
`kernel=`*`FILEPATH`*	Sets the kernel path to *`FILEPATH`*.
`kernelopt=`*`STRING`*	Appends *`STRING`* to the kernel boot options.
`modules=`*`FILEPATH1`* `---` *`FILEPATH2`*`... ---` *`FILEPATHn`*	Lists the modules to be loaded, separated by three hyphens (---).

See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 45, "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 49, "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 51, and "PXE Booting the ESXi Installer," on page 46.

Install or Upgrade ESXi from a CD or DVD by Using a Script

You can install or upgrade ESXi from a CD-ROM or DVD-ROM drive by 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 45.

Prerequisites

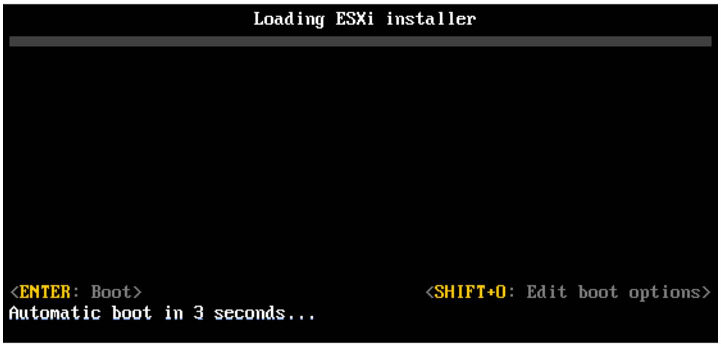
Before you run the scripted installation or upgrade, verify that the following prerequisites are met:

- The system on which you are installing or upgrading meets the hardware requirements. See "ESXi Hardware Requirements," on page 23.
- You have the ESXi installer ISO on an installation CD or DVD . See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 42.
- 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 60.
- You have selected a boot command to run the scripted installation or upgrade. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 58. For a complete list of boot commands, see "Boot Options," on page 59.

Procedure

1 Boot the ESXi installer from the local CD-ROM or DVD-ROM drive.

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



```
Loading ESXi installer

<ENTER: Boot>                              <SHIFT+O: Edit boot options>
Automatic boot in 3 seconds...
```

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 or Upgrade ESXi from a USB Flash Drive by Using a Script

You can install or upgrade ESXi from a USB flash drive by using a script that specifies the installation or upgrade options.

Supported boot options are listed in "Boot Options," on page 59.

Prerequisites

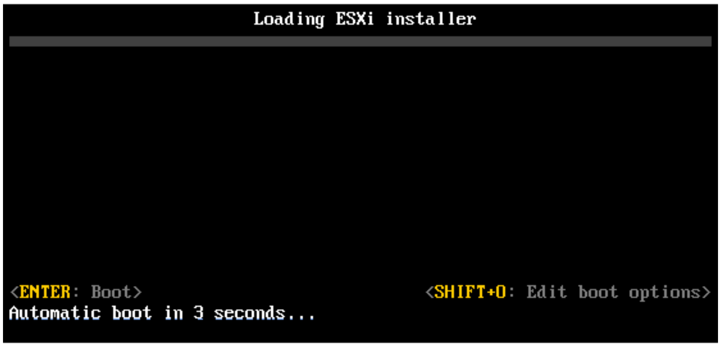
Before running the scripted installation or upgrade, verify that the following prerequisites are met:

- The system that you are installing or upgrading to ESXi meets the hardware requirements for the installation or upgrade. See "ESXi Hardware Requirements," on page 23.
- 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 42.
- 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 60.
- 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 58.

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.



```
                    Loading ESXi installer

<ENTER: Boot>                       <SHIFT+O: Edit boot options>
Automatic boot in 3 seconds...
```

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 Using PXE to Boot the Installer

ESXi 6.0 provides many options for using PXE to boot 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 46.
- For information about creating and locating an installation script, see "About Installation and Upgrade Scripts," on page 60.
- For specific procedures to use PXE to 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 51
  - "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 49
  - "PXE Boot the ESXi Installer Using gPXE," on page 52
- For information about using vSphere Auto Deploy to perform a scripted installation by using PXE to boot, see "Installing ESXi Using vSphere Auto Deploy," on page 71.

Installing ESXi Using vSphere Auto Deploy

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

Using Auto Deploy, experienced system administrators can manage large deployments efficiently. Hosts are network-booted from a central Auto Deploy server. Optionally, hosts are configured with a host profile of a reference host. The host profile can be set up to prompt the user for input. After boot up and configuration complete, the hosts are managed by vCenter Server just like other ESXi hosts.

Auto Deploy can also be used for stateless caching or stateful installs.

IMPORTANT Auto Deploy requires a secure separation between the production network and the management or deployment networks as discussed in "Auto Deploy Security Considerations," on page 116. Using Auto Deploy without this separation is insecure.

Stateless caching

By default, Auto Deploy does not store ESXi configuration or state on the host disk. Instead, an image profile defines the image that the host is provisioned with, and other host attributes are managed through host profiles. A host that uses Auto Deploy for stateless caching still needs to connect to the Auto Deploy server and the vCenter Server.

Stateful installs

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

Understanding vSphere Auto Deploy

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

Introduction to Auto Deploy

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

State Information for ESXi Hosts

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

Table 4-5. Auto Deploy Stores Information for Deployment

Information Type	Description	Source of Information
Image state	The executable software to run on an ESXi host.	Image profile, created with Image Builder PowerCLI.
Configuration state	The 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	The runtime state that is generated by the running software, for example, generated private keys or runtime databases.	Host memory, lost during reboot.

Table 4-5. Auto Deploy Stores Information for Deployment (Continued)

Information Type	Description	Source of Information
Virtual machine state	The virtual machines stored on a host and virtual machine autostart information (subsequent boots only).	Virtual machine information sent by vCenter Server to Auto Deploy must be available to supply virtual machine information to Auto Deploy.
User input	State that is based on user input, for example, an IP address that the user provides when the system starts up, cannot automatically be included in the host profile.	Host customization information, stored by vCenter Server during first boot. You can create a host profile that requires user input for certain values. When Auto Deploy applies a host profile that requires user provided information, the host is placed in maintenance mode. Use the host profile UI to check the host profile compliance, and respond to the prompt to customize the host.

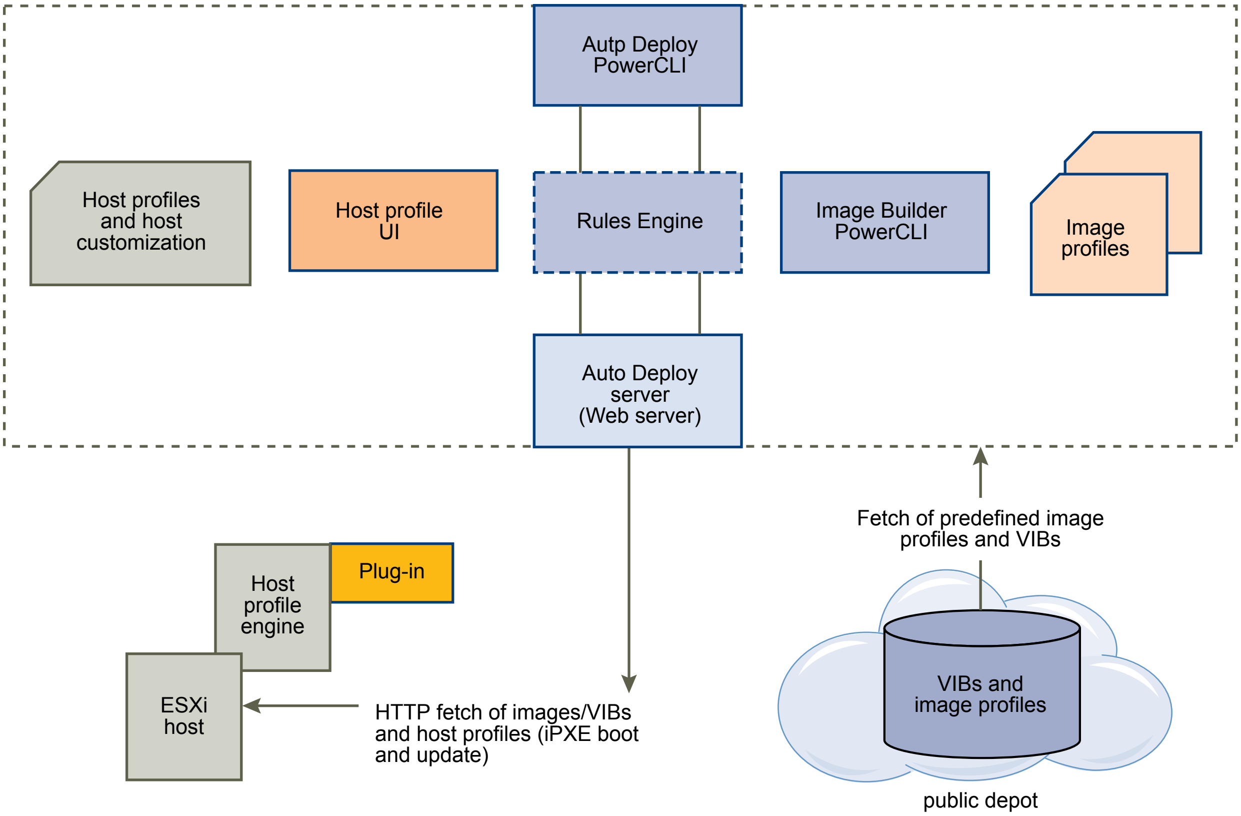
Auto Deploy Architecture

The Auto Deploy infrastructure consists of several components.

For more information, watch the video "Auto Deploy Architecture":

Auto Deploy Architecture (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_auto_deploy_architecture)

Figure 4-1. vSphere Auto Deploy Architecture


Autp Deploy PowerCLI
Host profiles and host customization
Host profile UI
Rules Engine
Image Builder PowerCLI
Image profiles
Auto Deploy server (Web server)
Fetch of predefined image profiles and VIBs
Host profile engine
Plug-in
ESXi host
HTTP fetch of images/VIBs and host profiles (iPXE boot and update)
VIBs and image profiles
public depot

Auto Deploy server

Serves images and host profiles to ESXi hosts.

Auto Deploy rules engine

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

Image profiles

Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use the Image Builder PowerCLI to examine the depot, and use the Auto Deploy rules engine to specify which image profile to assign to which host.
- VMware customers can create a custom image profile based on the public image profiles and VIBs in the depot and apply that image profile to the host. See "Using vSphere ESXi Image Builder," on page 137.

Host profiles

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

Host customization

Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. See "Host Customization in the vSphere Web Client," on page 109.

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

Rules and Rule Sets

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

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

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

The rules engine includes rules and rule sets.

Rules

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

Active Rule Set

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

Working Rule Set

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

You use the following workflow with rules and rule sets.

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

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

See the PowerCLI command-line help and "Managing Auto Deploy with PowerCLI Cmdlets," on page 87.

Auto Deploy Boot Process

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

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

First Boot Prerequisites

Before a first boot process, you must set up your system. Setup includes the following tasks, which are discussed in more detail in "Preparing for vSphere Auto Deploy," on page 82.

- Set up a DHCP server that assigns an IP address to each host upon startup and that points the host to the TFTP server to download the iPXE boot loader from.
- Verify 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. See "Setting Up an Auto Deploy Reference Host," on page 101.
- Specify rules for the deployment of the host and add the rules to the active rule set.

First Boot Overview

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

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

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

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

3. iPXE starts executing.

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

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

   a. Queries the rules engine for information about the host.

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

5. The host boots using the image profile.

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

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

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

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

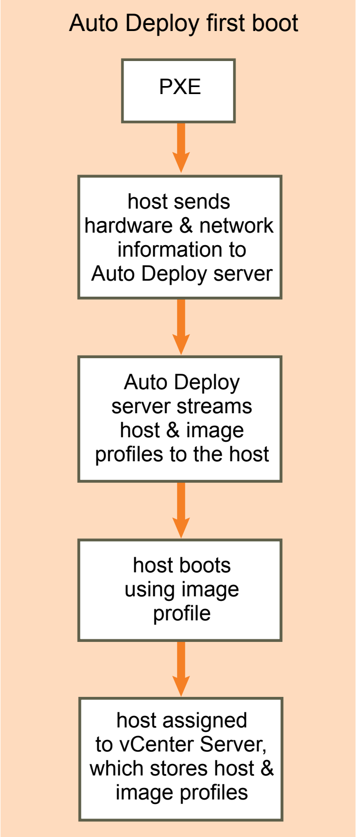
7 (Optional) If the host profile requires the user to specify certain information, such as a static IP address, the host is placed in maintenance mode when the host is added to the vCenter Server system.

  You must reapply the host profile and update the host customization to have the host exit maintenance mode. When you update the host customization, answer any questions when prompted.

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

See "Provision a Host (First Boot)," on page 91.

Figure 4-2. Auto Deploy Installation, First Boot


Auto Deploy first boot
PXE
host sends hardware & network information to Auto Deploy server
Auto Deploy server streams host & image profiles to the host
host boots using image profile
host assigned to vCenter Server, which stores host & image profiles

Subsequent Boots Without Updates

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

1 The administrator reboots the host.

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

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

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

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

Auto Deploy cannot set up vSphere distributed switches if vCenter Server is unavailable, and virtual machines are assigned to hosts only if they participate in an HA cluster. Until the host is reconnected to vCenter Server and the host profile is applied, the switch cannot be created. Because the host is in maintenance mode, virtual machines cannot start. See "Reprovision Hosts with Simple Reboot Operations," on page 92.

Any hosts that are set up to require user input are placed in maintenance mode. See "Update the Host Customization in the vSphere Web Client," on page 94.

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 Quick Start," on page 79 for an example.

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

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

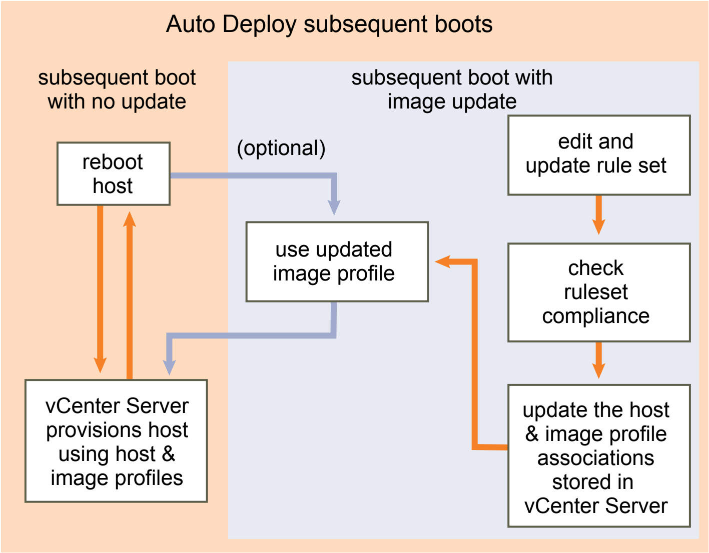
4 The administrator runs the `Repair-DeployRulesetCompliance` cmdlet to update the image profile, host profile, or vCenter Server location the vCenter Server system stores for each host.

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

   If the host profile is set up to request user input, the host is placed in maintenance mode. Follow the steps in "Update the Host Customization in the vSphere Web Client," on page 94.

See "Test and Repair Rule Compliance," on page 90.

Figure 4-3. Auto Deploy Installation, Subsequent Boots


Auto Deploy subsequent boots
subsequent boot with no update
subsequent boot with image update
reboot host
(optional)
edit and update rule set
use updated image profile
check ruleset compliance
vCenter Server provisions host using host & image profiles
update the host & image profile associations stored in vCenter Server

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 Quick Start 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 Quick Start

Getting started with Auto Deploy requires that you learn how Auto Deploy works, install the Auto Deploy server, install vSphere PowerCLI, write vSphere PowerCLI rules that provision hosts, and power on your hosts to be booted with the image profile you specify. You can customize of the image profile, host profile, and vCenter Server location.

See "Auto Deploy Proof of Concept Setup," on page 124 for a step-by-step exercise that helps you set up your first Auto Deploy environment on a Windows Server 2008 system.

To provision the hosts in your environment with Auto Deploy successfully, you can follow these steps.

1. Install vCenter Server and the vCenter Server components, or deploy the vCenter Server Appliance.

   The Auto Deploy server is included with the management node.

2. Install vSphere PowerCLI, which includes Auto Deploy and Image Builder cmdlets.

   See "Install vSphere PowerCLI and Prerequisite Software," on page 84 and "Using Auto Deploy Cmdlets," on page 85.

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

   - In most cases, you add the depots containing the required software to your vSphere 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 vSphere PowerCLI session.

   You must use Image Builder for customization 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 vSphere PowerCLI session as a URL.

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

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

   See "Assign an Image Profile to Hosts," on page 87.

   Note Auto Deploy is optimized for provisioning hosts that have a fixed MAC address to IP address mapping in DHCP (sometimes called DHCP reservations). If you want to use static IP addresses, you must set up the host profile to prompt for host customization. See "Set Up Host Profiles for Static IP Addresses in the vSphere Web Client," on page 108.

5 Power 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 101.

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

See the *Host Profiles* documentation.

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

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

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

Where *my_host_profile_from_reference_host* is the name of the reference host profile, and *my_target_cluster* is the name of the target cluster.

9 Power on the hosts that 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 Verify that the hosts you provisioned meet the following requirements.

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

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

Read "Understanding vSphere Auto Deploy," on page 72 for an introduction to the boot process, differences between first and subsequent boots, and an overview of using host customization.

Auto Deploy PowerCLI Cmdlet Overview

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

If you are new to PowerCLI, read the PowerCLI documentation and review "Using Auto Deploy Cmdlets," on page 85. 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 4-6. Rule Engine PowerCLI Cmdlets

Command	Description
`Get-DeployCommand`	Returns a list of Auto Deploy cmdlets.
`New-DeployRule`	Creates a new rule with the specified items and patterns.

Table 4-6. Rule Engine PowerCLI Cmdlets (Continued)

Command	Description
`Set-DeployRule`	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set.
`Get-DeployRule`	Retrieves the rules with the specified names.
`Copy-DeployRule`	Clones and updates an existing rule.
`Add-DeployRule`	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the `NoActivate` parameter to add a rule only to the working rule set.
`Remove-DeployRule`	Removes one or more rules from the working rule set and from the active rule set. Run this command with the `–Delete` parameter to completely delete the rule.
`Set-DeployRuleset`	Explicitly sets the list of rules in the working rule set.
`Get-DeployRuleset`	Retrieves the current working rule set or the current active rule set.
`Switch-ActiveDeployRuleset`	Activates a rule set so that any new requests are evaluated through the rule set.
`Get-VMHostMatchingRules`	Retrieves rules matching a pattern. For example, you can retrieve all rules that apply to a host or hosts. Use this cmdlet primarily for debugging.
`Test-DeployRulesetCompliance`	Checks whether the items associated with a specified host are in compliance with the active rule set.
`Repair-DeployRulesetCompliance`	Given the output of `Test-DeployRulesetCompliance`, this cmdlet updates the image profile, host profile, and location for each host in the vCenter Server inventory. The cmdlet might apply image profiles, apply host profiles, or move hosts to prespecified folders or clusters on the vCenter Server system.
`Apply-EsxImageProfile`	Associates the specified image profile with the specified host.
`Get-VMHostImageProfile`	Retrieves the image profile in use by a specified host. This cmdlet differs from the `Get-EsxImageProfile` cmdlet in the Image Builder PowerCLI.
`Repair-DeployImageCache`	Use this cmdlet only if the Auto Deploy image cache is accidentally deleted.
`Get-VMHostAttributes`	Retrieves the attributes for a host that are used when the Auto Deploy server evaluates the rules.
`Get-DeployMachineIdentity`	Returns a string value that Auto Deploy uses to logically link an ESXi host in vCenter to a physical machine.
`Set-DeployMachineIdentity`	Logically links a host object in the vCenter Server database to a physical machine. Use this cmdlet to add hosts without specifying rules.
`Get-DeployOption`	Retrieves the Auto Deploy global configuration options. This cmdlet currently supports the `vlan-id` option, which specifies the default VLAN ID for the ESXi Management Network of a host provisioned with Auto Deploy. Auto Deploy uses the value only if the host boots without a host profile.
`Set-DeployOption`	Sets the value of a global configuration option. Currently supports the `vlan-id` option for setting the default VLAN ID for the ESXi Management Network.

Preparing for vSphere Auto Deploy

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

- Prepare Your System and Install the Auto Deploy Server on page 82

  Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that Auto Deploy interacts with.

- Install vSphere PowerCLI and Prerequisite Software on page 84

  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 vSphere PowerCLI installation.

- Using Auto Deploy Cmdlets on page 85

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

- Set Up Bulk Licensing on page 85

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

Prepare Your System and Install the Auto Deploy Server

Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that Auto Deploy interacts with.

Prerequisites

- Verify that the hosts that you plan to provision with Auto Deploy meet the hardware requirements for ESXi. See "ESXi Hardware Requirements," on page 23.

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

- Verify that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met. See "vCenter Server Required Ports," on page 33.

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

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

- 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.
- 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, set up your first host so that 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 103.
- Verify that the Auto Deploy server has an IPv4 address. Auto Deploy does not support a pure IPv6 environment end-to-end. The PXE boot infrastructure does not support IPv6. After the deployment you can manually reconfigure the hosts to use IPv6 and add them to vCenter Server over IPv6. However, when you reboot a stateless host, its IPv6 configuration is lost.

Procedure

1 Install vCenter Server or deploy the vCenter Server Appliance.

The Auto Deploy server is included with the management node.

2 Configure the Auto Deploy service startup type.

a Log in to your vCenter Server system by using the vSphere Web Client.

b On the vSphere Web Client Home page, click **Administration**.

c Under **System Configuration** click **Services**.

d Select **Auto Deploy**, click the **Actions** menu, and select **Edit Startup Type**.

- On Windows, the Auto Deploy service is disabled. In the Edit Startup Type window, select **Manual** or **Automatic** to enable Auto Deploy.
- On the vCenter Server Appliance, the Auto Deploy service by default is set to **Manual**. If you want the Auto Deploy service to start automatically upon OS startup, select **Automatic**.

3 Configure the TFTP server.

a In a vSphere Web Client connected to the vCenter Server system, go to the inventory list and select the vCenter Server system.

b Click the **Manage** tab, select **Settings**, and click **Auto Deploy**.

c Click **Download TFTP Boot Zip** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.

4 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`.

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

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

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

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

8 (Optional) If you set up your environment to use Thumbprint mode, 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/`.

   By default, vCenter Server 6.0 and later uses vSphere Certificate Authority.

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

What to do next

- Install vSphere PowerCLI. See "Install vSphere PowerCLI and Prerequisite Software," on page 84.
- Use the vSphere PowerCLI cmdlets to define a rule that assigns an image profile and optional host profile to the host.
- (Optional) Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- If you want to have Auto Deploy overwrite existing partitions, set up a reference host to do auto partitioning and apply the host profile of the reference host to other hosts. See "Consider and Implement Your Partitioning Strategy," on page 107.
- If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. See "Host Customization in the vSphere Web Client," on page 109.

Install vSphere 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 vSphere 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 User's Guide* for detailed instructions for vSphere PowerCLI installation.

Prerequisites

- Verify that Microsoft .NET 4.5 SP2 is installed, or install it from the Microsoft Web site following the instructions on that Web site.
- Verify that Windows PowerShell 3.0 is installed, or install it from the Microsoft Web site following the instructions on that Web site.

Procedure

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

What to do next

Review "Using Auto Deploy Cmdlets," on page 85. If you are new to vSphere PowerCLI, read the vSphere PowerCLI documentation.

Use Auto Deploy cmdlets and other vSphere PowerCLI cmdlets and PowerShell cmdlets to manage Auto Deploy rules and rule sets. Use `Get-Help`*`cmdlet_name`* 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 vSphere PowerCLI features.

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

You can type cmdlets, parameters, and parameter values in the vSphere 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 `flfl` or `ft`. For more information, run the `Get-Help Format-List` cmdlet.

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 *vSphere Installation and Setup* documentation pass in parameters by name.

Passing Parameters as Objects

You can pass parameters as objects if you want to perform 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. View 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 using the `Repair-DeployRuleSetCompliance` cmdlet with the variable.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

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

Set Up Bulk Licensing

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

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

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

Prerequisites

Install PowerCLI. See "Install vSphere PowerCLI and Prerequisite Software," on page 84.

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

Assign license keys with the vSphere Web Client
You can assign license keys to a host when you add the host to the vCenter Server system or when the host is managed by a vCenter Server system.

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Managing Auto Deploy with PowerCLI Cmdlets

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

Assign an Image Profile to Hosts

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

Auto Deploy extensibility rules enforce that VIBs at the CommunitySupported level can only contain files from certain predefined locations, such as the ESXCLI plug-in path, jumpstart plug-in path, and so on. If you add a VIB that is in a different location to an image profile, a warning results. You can override the warning by using the `force` option.

If you call the `New-DeployRule` cmdlet on an image profile that includes VIBs at the CommunitySupported level which violate the rule, set `$DeployNoSignatureCheck = $true` before adding the image profile. With that setting, the system ignores signature validation and does not perform the extensibility rules check.

NOTE Image profiles that include VIBs at the CommunitySupported level are not supported on production systems.

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 85.

Procedure

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

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

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

2 Determine the location of a public software depot, or define a custom image profile using the Image Builder PowerCLI.

3 Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path. b Run **`Add-EsxSoftwareDepot C:\`*****`file_path`*****`\`*****`my_offline_depot`*****`.zip`**.

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

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

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

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

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

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

6. Add the rule to the rule set.

   ```
   Add-DeployRule testrule
   ```

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

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

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

What to do next

- For hosts already provisioned with Auto Deploy, perform the compliance testing and repair operations to provision them with the new image profile. See "Test and Repair Rule Compliance," on page 90.
- Turn on unprovisioned hosts to provision them with the new image profile.

Write a Rule and 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.

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. See "Install vSphere PowerCLI and Prerequisite Software," on page 84.
- Export the host profile that you want to use.

Procedure

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

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

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

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

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

4 At the vSphere PowerCLI prompt, define a rule in which host profiles are assigned to hosts with certain attributes, for example a range of IP addresses.

```
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

- Assign a host already provisioned with Auto Deploy to the new host profile by performing compliance test and repair operations on those hosts. For more information, see "Test and Repair Rule Compliance," on page 90.
- Power on unprovisioned hosts to provision them with the host profile.

Write a Rule and 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.

Prerequisites

- Install vSphere PowerCLI and all the prerequisite software.
- Verify that the folder you select is in a data center or in a cluster. You cannot assign the host to a standalone top-level folder.

Procedure

1 Run the `Connect-VIServer` vSphere 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 appear. 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 data center 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

- Assign a host already provisioned with Auto Deploy to the new folder or cluster location by performing test and repair compliance operation. See "Test and Repair Rule Compliance," on page 90.
- Power 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.

Prerequisites

- Install vSphere PowerCLI and all prerequisite software.
- Verify that your infrastructure includes one or more ESXi hosts provisioned with Auto Deploy, and that the host on which you installed vSphere PowerCLI can access those ESXi hosts.

Procedure

1 Use vSphere 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 can 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 you can access the host for which you want to test rule set compliance.

```
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 the contents of the rule set and configuration of the host.

```
$tr.itemlist
```

The system returns a table of current and expected items.

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

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

```
Repair-DeployRuleSetCompliance $tr
```

What to do next

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

Provisioning ESXi Systems with vSphere Auto Deploy

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

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

Provision a Host (First Boot)

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

Prerequisites

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

  See "ESXi Hardware Requirements," on page 23.

- Prepare the system for vSphere Auto Deploy (see "Preparing for vSphere Auto Deploy," on page 82).

- 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 87.

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

Procedure

1 Turn on the host.

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

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

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

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

What to do next

Reprovision hosts as needed. See "Reprovisioning Hosts," on page 92.

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 90.

Reprovisioning Hosts

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

A first boot using Auto Deploy requires that you set up your environment and add rules to the rule set. See "Preparing for vSphere Auto Deploy," on page 82.

The following reprovisioning operations are available.

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

Reprovision Hosts with Simple Reboot Operations

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

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

Prerequisites

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

Procedure

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

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

3. Reboot the host.

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

Reprovision a Host with a New Image Profile

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

Several options for reprovisioning hosts exist.

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

Prerequisites

- Create the image profile you want to boot the host with. Use the Image Builder PowerCLI, discussed in "Using vSphere ESXi Image Builder," on page 137.
- Make sure that the setup that you performed during the first boot operation is in place.

Procedure

1 At the PowerShell prompt, run the `Connect-VIServer` PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

  `Connect-VIServer myVCServer`

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

2 Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with the Image Builder PowerCLI.

3 Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine. b Run **`Add-EsxSoftwareDepot C:\`*`file_path`*`\`*`my_offline_depot`*`.zip`**.

4 Run `Get-EsxImageProfile` to see a list of image profiles, and decide which profile you want to use.

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

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

  `Copy-DeployRule myrule -ReplaceItem` ***`my_new_imageprofile`***

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

  See "Test and Repair Rule Compliance," on page 90.

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

Update the Host Customization in the vSphere Web Client

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

Prerequisites

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

Procedure

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

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

2 In the vSphere Web Client, right click the host and click **All vCenter Actions > Host Profiles > Remediate** to remediate the host.

3 When prompted, provide the user input.

You can now direct the host to exit maintenance mode.

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

Using Auto Deploy for Stateless Caching and Stateful Installs

The Auto Deploy stateless caching feature lets you cache the host's image. The Auto Deploy stateful installs feature lets you install hosts over the network. After the initial network boot, these hosts boot like other ESXi hosts.

The stateless caching solution is primarily intended for situations when several hosts boot simultaneously. The locally cached image helps prevent a bottleneck that results if several hundreds of hosts connect to the Auto Deploy server simultaneously. After the boot operation is complete, hosts connect to Auto Deploy to complete the setup.

The stateful installs feature lets you provision hosts with the image profile over the network without having to set up the PXE boot infrastructure.

- Introduction to Stateless Caching and Stateful Installs on page 95

  You can use the System Cache Configuration host profile to provision hosts with Auto Deploy stateless caching and stateful installs.

- Understanding Stateless Caching and Stateful Installs on page 96

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

- Set Up Stateless Hosts to Use Auto Deploy with Caching on page 97

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

- Enable Stateful Installs for Hosts Provisioned with Auto Deploy on page 99

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

Introduction to Stateless Caching and Stateful Installs

You can use the System Cache Configuration host profile to provision hosts with Auto Deploy stateless caching and stateful installs.

Examples of Stateless Caching and Stateful Installs

Hosts provisioned with Auto Deploy cache the image (stateless caching)

Set up and apply a host profile for stateless caching. You can cache the image on a local disk, a remote disk, or a USB drive. Continue provisioning this host with Auto Deploy. If the Auto Deploy server becomes unavailable, for example because hundreds of hosts attempt to access it simultaneously, the host boots from the cache. The host attempts to reach the Auto Deploy server after the boot operation to complete configuration.

Hosts provisioned with Auto Deploy become stateful hosts

Set up and apply a host profile for stateful installs. When you provision a host with Auto Deploy, the image is installed on the local disk, a remote disk, or a USB drive. For subsequent boots, you boot from the disk. The host no longer uses Auto Deploy.

Preparation

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

Table 4-7. Preparation for Stateless Caching or Stateful Installs

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

Stateless Caching and Loss of Connectivity

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

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

Understanding Stateless Caching and Stateful Installs

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

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

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

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

Using the vSphere Web Client to Set Up Auto Deploy for Stateless Caching or Stateful Installs

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

1. You provision a host with Auto Deploy and edit that host's System Image Cache Configuration host profile.
2. You place one or more target hosts in maintenance mode, apply the host profile to each host, and instruct the host to exit maintenance mode.
3. What happens next depends on the host profile you selected.
   - If the host profile enabled stateless caching, the image is cached to disk. No reboot is required.
   - If the host profile enabled stateful installs, the image is installed. When you reboot, the host uses the installed image.
4. A reboot is required so the changes can take effect.

Using PowerCLI to Set Up Auto Deploy for Stateless Caching or Stateful Installs

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

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

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

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

- For stateful installs, Auto Deploy proceeds as follows:
  - During first boot, Auto Deploy installs the image on the host.
  - During subsequent boots, the host boots from disk. Auto Deploy is no longer involved.
- For stateless caching, Auto Deploy proceeds as follows:
  - During first boot, Auto Deploy provisions the host and caches the image.
  - During subsequent boots, Auto Deploy provisions the host. If Auto Deploy is unavailable, the host boots from the cached image, however, setup can only be completed when the host can reach the Auto Deploy server.

Set Up Stateless Hosts to Use Auto Deploy with Caching

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

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

Set up a highly available Auto Deploy infrastructure to guarantee that virtual machines are migrated to the host if the host reboots. Because vCenter Server assigns virtual machines to the host, vCenter Server must be available. See "Set Up Highly Available Auto Deploy Infrastructure," on page 115.

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

Table 4-8. Setting up hosts for stateless caching or stateful installs

Workflow	Stateless caching	Stateful install
Apply host profile directly	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. See "Configure a Host Profile to Use Stateless Caching," on page 98.	Apply the host profile either to individual hosts or to all hosts in a folder or cluster. See "Configure a Host Profile to Enable Stateful Installs," on page 100.
Write and apply PowerCLI rules	Set up a reference host with a host profile that has the caching setup you want. Write an Auto Deploy PowerCLI rule that provisions the host and that applies a host profile that is set up for stateless caching. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.	Set up a reference host with a host profile that has the caching setup you want. Write an Auto Deploy PowerCLI rule that provisions the host and that applies a host profile that is set up for stateful installs. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.

Prepare for Auto Deploy with Stateless Caching

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

Prerequisites

- Decide which disk to use for caching and determine whether the caching process will overwrite an existing VMFS partition.

- In production environments, protect the vCenter Server system and the Auto Deploy server by including them in a highly available environment. Having the vCenter Server in a management cluster guarantees that VDS and virtual machine migration are available. If possible, protect other elements of your infrastructure. See "Set Up Highly Available Auto Deploy Infrastructure," on page 115.

Procedure

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

  See "Preparing for vSphere Auto Deploy," on page 82.

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

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

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

  See your hardware vendor's documentation.

What to do next

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

Configure a Host Profile to Use Stateless Caching

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

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

Prerequisites

Prepare your host for stateless caching. See "Prepare for Auto Deploy with Stateless Caching," on page 97.

Procedure

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

  See the *Host Profiles* documentation.

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

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

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

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

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

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

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

Option	Description
Arguments for first disk	By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use **`esx`** for the first disk with ESX installed on it, use model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that uses the mptsas driver, and third for the local disk, specify **`ST3120814A,mptsas,local`** as the value of this field. The first disk setting in the host profile specifies the search order for determining which disk to use for the cache. The search order is specified as a comma delimited list of values. The default setting **`esx,local`** specifies that Auto Deploy should first look for an existing cache disk. The cache disk is identified as a disk with an existing ESXi software image. If Auto Deploy cannot find an existing cache disk, it searches for an available local disk device. When searching for an available disk Auto Deploy uses the first empty disk that does not have an existing VMFS partition. You can use the first disk argument only to specify the search order. You cannot explicitly specify a disk. For example, you cannot specify a specific LUN on a SAN.
Check to overwrite any VMFS volumes on the selected disk	If you click this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.

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

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

Option	Description
vSphere Web Client	Use the host profiles interface of the vSphere Web Client. See the *Host Profiles* documentation.
vSphere PowerCLI	See "Write a Rule and Assign a Host Profile to Hosts," on page 88.

Enable Stateful Installs for Hosts Provisioned with Auto Deploy

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

Prepare Hosts Provisioned with Auto Deploy for Stateful Installs

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

Prerequisites

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

Procedure

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

See "Preparing for vSphere Auto Deploy," on page 82.

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

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

3 Set up the host to boot from disk.

See your hardware vendor's documentation.

Configure a Host Profile to Enable Stateful Installs

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

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

Prerequisites

Make sure that your host is configured for Auto Deploy and that you meet other prerequisites for stateful installs. See "Prepare Hosts Provisioned with Auto Deploy for Stateful Installs," on page 99.

Procedure

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

See the *Host Profiles* documentation.

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

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

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

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

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

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

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

Option	Description
Arguments for first disk	By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use **`esx`** for the first disk with ESX installed on it, use model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that uses the mptsas driver, and third for the local disk, specify **`ST3120814A,mptsas,local`** as the value of this field. The first disk setting in the host profile specifies the search order for determining which disk to use for the cache. The search order is specified as a comma delimited list of values. The default setting **`esx,local`** specifies that Auto Deploy should first look for an existing cache disk. The cache disk is identified as a disk with an existing ESXi software image. If Auto Deploy cannot find an existing cache disk, it searches for an available local disk device. When searching for an available disk Auto Deploy uses the first empty disk that does not have an existing VMFS partition. You can use the first disk argument only to specify the search order. You cannot explicitly specify a disk. For example, you cannot specify a specific LUN on a SAN.
Check to overwrite any VMFS volumes on the selected disk	If you click this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.

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

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

Option	Description
vSphere Web Client	To apply the host profile to individual hosts, use the host profiles interface of the vSphere Web Client. See the *Host Profiles* documentation.
vSphere PowerCLI	To apply the host profile to one or more hosts by using PowerCLI, see "Write a Rule and Assign a Host Profile to Hosts," on page 88.

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 setup might also include security, storage, networking, and ESXi Dump Collector. You can apply such a host's setup to other hosts by using host profiles.

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

NTP Server Setup

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

Syslog Server Setup

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

Core Dump Setup

You can set up your reference host to send core dumps to a shared SAN LUN, or you can install ESXi Dump Collector in your environment and configure the reference host to use ESXi Dump Collector. See "Configure ESXi Dump Collector with ESXCLI," on page 103. 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 to access 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 to use Active Directory.

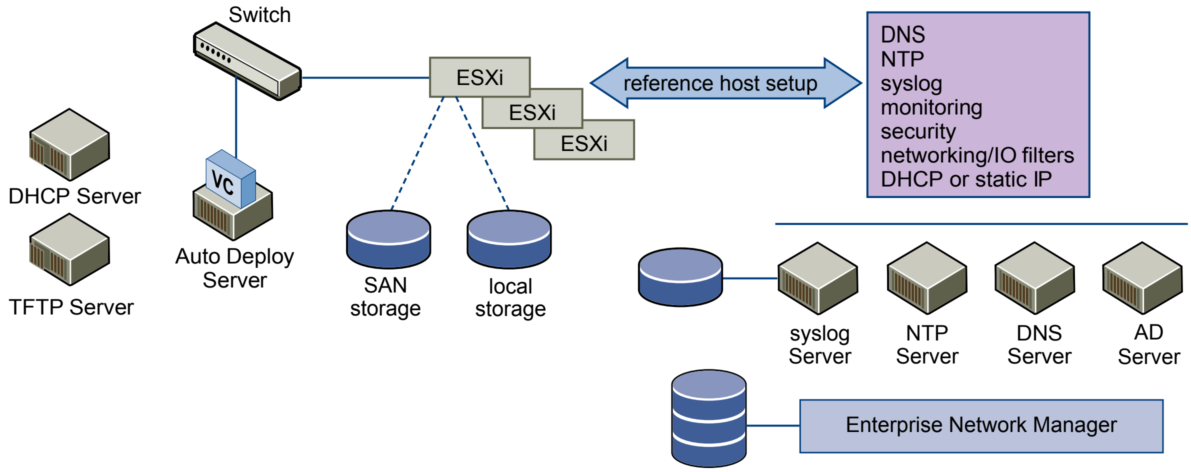
Note If you set up Active Directory by using host profiles, the passwords are not protected. Use the vSphere Authentication Service to set up Active Directory to avoid exposing the Active Directory password.

Networking and Storage Setup

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

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

Figure 4-4. Auto Deploy Reference Host Setup



"Configuring an Auto Deploy Reference Host," on page 103 explains how to perform this setup.

Watch the video "Auto Deploy Reference Hosts" for information about the reference host setup:

Auto Deploy Reference Hosts (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_auto_deploy_reference_hosts)

Configuring an Auto Deploy Reference Host

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

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

vSphere Web Client

The vSphere Web Client supports setup of networking, storage, security, and most other aspects of anESXi host. Set up your environment and create a host profile from the reference host for use by Auto Deploy.

vSphere Command-Line Interface

You can use vCLI commands for setup of many aspects of your host. vCLI is suitable for configuring many of the services in the vSphere environment. Commands include `vicfg-ntp` (set up an NTP server), `esxcli system syslog` (set up a syslog server), and `esxcli network route` (add routes and set up the default route). See "Configure ESXi Dump Collector with ESXCLI," on page 103.

Host Profiles Interface

Best practice is to set up a host with vSphere Web Client or vCLI and create a host profile from that host. You can instead use the Host Profiles interface in the vSphere Web Client and save that host profile. See "Configure Host Profiles for an Auto Deploy Reference Host with the vSphere Web Client," on page 104.

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.

If you intend to use IPv6, and if both the ESXi host and ESXi Dump Collector are on the same local link, both can use either local link scope IPv6 addresses or global scope IPv6 addresses.

If you intend to use IPv6, and if ESXi and ESXi Dump Collector are on different hosts, both require global scope IPv6 addresses. The traffic routes through the default IPv6 gateway.

Prerequisites

- ESXi Dump Collector is included with the vCenter Server management node.
- 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-ip 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. You can use an IPv4 address or an IPv6 address. If you configure an ESXi system that is running on a virtual machine that is using a vSphere standard switch, you must select a VMkernel port that is in promiscuous mode.

2. Enable ESXi Dump Collector.

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

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

   ```
   esxcli system coredump network check
   ```

The host on which you have set up ESXi Dump Collector is configured 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 specified in the reference host. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.
- 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 90.
- Power on unprovisioned hosts to provision them with the new host profile.

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

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

Prerequisites

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

Procedure

1. In the vSphere Web Client, click **Rules and Profiles** and click **Host Profiles**.
2. For a new profile, click the **Create Profile from a host** icon, or right-click a profile that you want to modify and select **Edit Host Profile**.

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

Policy	Description
ESXi Dump Collector	Set up ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (best practice), or configure the host profile directly. See "Set Up Syslog from the Host Profiles Interface in the vSphere Web Client," on page 106.
Syslog	Set up syslog for the host with the `esxcli system syslog` command. Save the host profile (best practice) or configure the host profile directly. See "Set Up Syslog from the Host Profiles Interface in the vSphere Web Client," on page 106.
NTP	Use the `vicfg-ntp` vCLI command or the vSphere Web Client to set up a host. If you use the vSphere Web Client to start the NTP Server, make sure the startup policy for the NTP Daemon is set appropriately. a In the vSphere Web Client, select the host. b Select the Manage tab and click **Time Configuration**. c Click **Edit** and click Use Network Time Protocol (Enable NTP client). d Select **Start and stop with host** as the NTP Service Startup Policy.
Security	Set up the firewall configuration, security configuration, user configuration, and user group configuration for the reference host with the vSphere Web Client or with vCLI commands. See the *vSphere Security* documentation.
Networking and Storage	Set up the networking and storage policies for the reference host with the vSphere Web Client or vCLI command.

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

What to do next

Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Write a Rule and Assign a Host Profile to Hosts," on page 88). Perform a test-and-repair compliance operation.

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

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

Best practice is to set up hosts to use ESXi Dump Collector with the `esxcli system coredump` command and save the host profile (see "Configure ESXi Dump Collector with ESXCLI," on page 103). If you prefer to use a GUI, set up ESXi Dump Collector from the Host Profiles interface.

Prerequisites

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

Procedure

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

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

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

4 Select **Network Configuration**.

5 Select **Network Coredump Settings**.

6 Click the **Enabled** check box.

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

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

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.
- 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 90.
- Turn on unprovisioned hosts to provision them with the new host profile.

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

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

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

Prerequisites

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

Procedure

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

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

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

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

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

   You can specify syslog settings from here.

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

   a Click the plus sign.

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

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

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

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

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host (see "Write a Rule and Assign a Host Profile to Hosts," on page 88).
- 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 90.
- Turn on unprovisioned hosts to provision them with the new image profile.

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

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

Prerequisites

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

Procedure

1. In the vSphere Web Client, select the host and click the **Networking** tab.
2. Perform networking setup.

   If you are using virtual switches and not vSphere Distributed Switch, do not add other VMkernel NICs to vSwitch0.
3. After the reference host is configured, reboot the system to verify that vmk0 is connected to the Management Network.
4. Create a host profile from the host.

What to do next

- Write a rule that applies the host profile to all hosts that you want to provision with the settings that you specified in the reference host. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.
- 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 90.
- Turn on unprovisioned hosts to provision them with the new host profile.

Consider and Implement Your Partitioning Strategy

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

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

To ensure that local SSDs remain unpartitioned during auto-partitioning, you must set the parameter **`skipPartitioningSsds=TRUE`** on the reference host.

For more information about preventing SSD formatting during auto-partitioning, see the *vSphere Storage* documentation.

Prerequisites

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

Procedure

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

2 Click **Settings**.

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

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

5 (Optional) If you want local SSDs to remain unpartitioned, scroll to `VMkernel.Boot.skipPartitioningSsds` and set the value to true.

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

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

Auto-partitioning is performed when the hosts boot.

Advanced Management Tasks

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

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

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

Prerequisites

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

Procedure

1 In the vSphere Web Client, navigate to the vCenter Server that manages the Auto Deploy host, select **Policies and Profiles**, and select **Host Profiles**.

2 Right-click the extracted host profile and click **Edit Settings**.

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

4 Change the default IP address settings by clicking **Networking configuration > Host port group > Management Network > IP address settings**.

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

6 If the host is in a different subnet than the vCenter Server system, select **Networking Configuration > NetStack Instance > defaultTcpipStack > DNS configuration** and enter the default route in the **Default IPv4 gateway** text box.

7 Select **Networking Configuration > NetStack Instance > defaultTcpipStack > DNS configuration**.

8 Make sure the **Flag indicating if DHCP should be used** check box is deselected.

9 Right-click the host and select **All vCenter Actions > Host Profiles > Attach Host Profile**.

10 Select the profile to attach and click **Next**.

11 Provide the IP address and net mask and click **Finish**.

12 Reboot the ESXi host.

The IP address is saved as a host customization and applied to the host.

Host Customization in the vSphere Web Client

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

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

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

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

Table 4-9. Host Profile Options that Prompt for iSCSI User Input

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

Table 4-10. Host Profile Options that Prompt for Storage User Input

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

Table 4-11. Host Profile Options that Prompt for Security User Input

Information to Request User Input For	Setting the Host Profile Option
Administrator password for ESXi host when the host boots for the first time.	1 Select **Edit Host Profile**, and click **Security and Services**. 2 click **Security Settings** and click **Security configuration**. 3 In the right panel, select **User Input Password to be Used to Configure Administrator Password** from the **Administrator password** drop-down menu.
Preconfigures a user for the ESXi host but prompts for the password for that user on each host when the host boots for the first time.	You can perform this task only if a user configuration already exists. Configure the user by selecting one of the options. ■ **Assigned fixed user configurations** is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear. ■ **Assign advanced fixed user configurations** is for users of ESXi 5.0 and later systems. ■ **Specify the user configuration in the profile but prompt for password during host configuration** allows you to specify the information about the user but prompt for a password on each host.
Prompt the user for credentials when the host joins the Active Directory domain.	1 Set the Authentication configuration profile to use a fixed domain. a Select **Edit Host Profile**, click **Security and Services**. b Click **Security Settings**, and click **Authentication configuration**. c Click **Active Directory configuration**. d In the Domain Name drop-down menu, select **Configure a fixed domain name**. 2 Set the method for joining the domain to prompt the user. a Select **Edit Host Profile**, click **Security and Services** and click **Authentication configuration**. b Click **Active Directory configuration**. c In the Join Domain Method drop-down menu, select **Use user specified AD credentials to join the host to domain**.

Table 4-12. Host Profile Options that Prompt for Networking User Input

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

Table 4-12. Host Profile Options that Prompt for Networking User Input (Continued)

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

Auto Deploy Best Practices and Security Consideration

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

Auto Deploy Best Practices

You can follow several Auto Deploy best practices, set up networking, configure vSphere HA, and otherwise optimize your environment for Auto Deploy.

See the VMware Knowledge Base for additional best practice information.

Auto Deploy and vSphere HA Best Practices

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

Some environments configure the hosts provisioned with Auto Deploy with a distributed switch or configure virtual machines running on the hosts with Auto Start Manager. In such environments, deploy the vCenter Server system so that its availability matches the availability of the Auto Deploy server. Several approaches are possible.

- In a proof of concept environment, deploy thevCenter Server system and the Auto Deploy server on the same system. In all other situations, install the two servers on separate systems.

- Deploy the vCenter Server system on 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 want 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. 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.

Auto Deploy and IPv6

Because Auto Deploy takes advantage of the iPXE infrastructure, it requires that each host has an IPv4 address. After the deployment you can manually reconfigure the hosts to use IPv6 and add them to vCenter Server over IPv6. However, when you reboot a stateless host, its IPv6 configuration is lost.

IP Address Allocation

Use DHCP reservations for address allocation. Fixed IP addresses are supported by the host customization mechanism, but providing input for each host is not recommended.

VLAN Considerations

Use Auto Deploy in environments that do not use VLANs.

If you intend to use Auto Deploy in an environment that uses VLANs, make sure that the hosts that 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 the router, or might be set in the host's BIOS or through the host profile. Contact your network administrator to determine the steps for allowing hosts to reach the DHCP server.

Auto Deploy and VMware Tools Best Practices

When you provision hosts with Auto Deploy, you can select an image profile that includes VMware Tools, or select the smaller image associated with the image profile that does not contain VMware Tools.

You can download two image profiles from the VMware download site.

- `xxxxx-standard`: An image profile that includes the VMware Tools binaries, required by the guest operating system running inside a virtual machine. The image is usually named esxi-*version*-*xxxxx*-standard.
- `xxxxx-no-tools`: An image profile that does not include the VMware Tools binaries. This image profile is usually smaller has a lower memory overhead, and boots faster in a PXE-boot environment. This image is usually named esxi-*version*-*xxxxx*-no-tools.

With vSphere 5.0 Update 1 and later, you can deploy ESXi using either image profile.

- If the network boot time is of no concern, and your environment has sufficient extra memory and storage overhead, use the image that includes VMware Tools.
- If you find the network boot time too slow when using the standard image, or if you want to save some space on the hosts, you can use the image profile that does not include VMware Tools, and place the VMware Tools binaries on shared storage. See, "Provision ESXi Host by Using an Image Profile Without VMware Tools," on page 117.

Auto Deploy Load Management Best Practices

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

Using Reverse Web Proxy Servers for Auto Deploy Scalability
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_reverse_web_proxy_for_auto_deploy_scalability)

Use multiple TFTP servers to point to different proxy servers. Use one TFTP server for each reverse proxy server. After that, set up the DHCP server to send different hosts to different TFTP servers.

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

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

vSphere Auto Deploy Logging and Troubleshooting Best Practices

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

Auto Deploy Logs

Download the Auto Deploy logs by going to the Auto Deploy page in the vSphere Web Client. See, "Download Auto Deploy Logs," on page 118.

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, enables network logging, and lets you combine 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 that 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 103.

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.

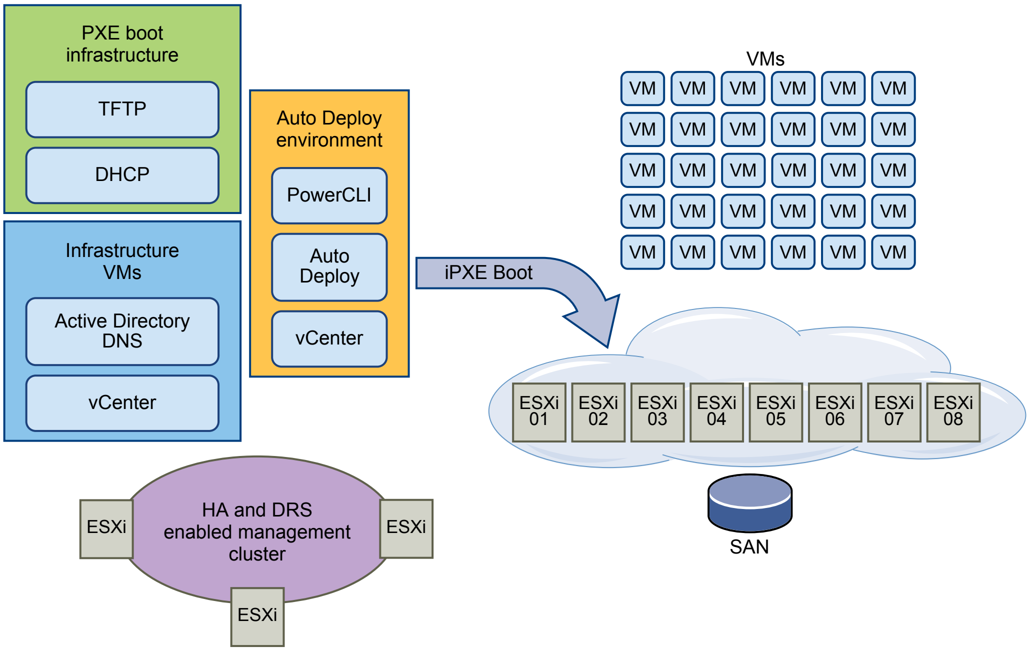
- Protect the Auto Deploy server. See "Auto Deploy and vSphere HA Best Practices," on page 112.
- Protect all other servers in your environment, including the DHCP server and the TFTP server.
- Follow VMware security guidelines, including those outlined in "Auto Deploy Security Considerations," on page 116.

Set Up Highly Available Auto Deploy Infrastructure

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

Highly Available Auto Deploy Infrastructure (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_ha_auto_deploy_infrastructure)

Figure 4-5. Highly Available Auto Deploy Infrastructure



Prerequisites

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

Watch the video "Highly Available Auto Deploy Infrastructure" for information about the implementation of a highly available Auto Deploy infrastructure:

Procedure

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

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

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

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

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

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

Auto Deploy Security Considerations

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

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

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

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

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

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

Using the Device Alias Configuration Host Profile

In vSphere 5.5 and later, you can persistently map a device (bus address) to a device name (alias). You can modify the mapping by using the Device Alias Configuration host profile. Using persistent mapping can help avoid compliance warnings for stateless hosts, and is also useful for stateful hosts.

The Device Alias Configuration host profile is selected by default, which means that aliases are assigned to each device. For example, if a host does not recognize one of the NICs during the boot process, the NIC aliases no longer change. That can help for management with scripts, and if you apply a host profile from a reference host.

NOTE To avoid errors, do not disable or edit the Device Alias Configuration host profile.

To ensure uniform, persistent, and stable device naming across all hosts, use the device alias profile with homogeneous hosts only. These are hosts that are identically configured with the same network and storage cards in the PCI bus.

NOTE Always bring the BIOS up to the latest level. For systems with earlier versions of the BIOS, the BIOS might not provide accurate location information for on-board devices. ESXi applies heuristics for this case to keep the alias stable, even for these devices, this might not work under all conditions, for example if changes are made in the BIOS setting or if the devices fail.

Device Alias Configuration Compliance Failures

For hosts are not fully homogenous, for example, the hosts contain different PCI cards or have different BIOS levels, if you apply the host profile from a reference host, a compliance check might result in a compliance failure. The compliance check ignores extra devices on the host that were not on the reference host. Select the host with the fewest devices as the reference host.

If the compliance check shows that he hosts are not fully homogeneous, the compliance failure cannot be remediated without modifying the hardware itself.

If the compliance check shows that the device aliases, for example, names such as vmhba3, are different from those on the reference host, remediation might be possible.

- To remediate a host that is not provisioned with Auto Deploy, perform host profile remediation and reboot the host.
- To remediate a host that is provisioned with Auto Deploy, reprovision a host.

Upgrading Systems for Device Alias Profiles

In ESXi versions earlier than 5.5, the Device Alias Configuration profile does not exist. Consider the following problems when you upgrade from previous versions of ESXi to ESXi 5.5:

- For installed hosts, that is, hosts not provisioned with Auto Deploy, upgrading the ESXi host preserves aliases. After they are upgraded, aliases remain stable as long as the BIOS provides the information.
- When you upgrade a cluster of ESXi host provisioned with Auto Deploy image, the aliases do not change because ESXi 5.5 uses the same algorithm to generate aliases as earlier versions. Generate a new host profile for the reference host. This host profile includes the Device Alias Configuration profile. Set up Auto Deploy to apply the reference host's host profile to all other hosts for consistent device naming across your cluster.
- When upgrading a system, do not flash the BIOS, because this action can change aliases. Flashing the BIOS to the latest level is more appropriate for a new install.

Provision ESXi Host by Using an Image Profile Without VMware Tools

When you provision ESXi hosts with Auto Deploy, you can select to provision the host by using the image profile that does not contain VMware Tools binaries. This image profile is usually smaller, has a lower memory overhead, and boots faster in a PXE-boot environment.

If you find the network boot time too slow when using the standard image, or if you want to save some space on the hosts, you can use the image profile that does not include VMware Tools, and place the VMware Tools binaries on a shared storage.

Prerequisites

Download the`xxxxx-no-tools` `image profile from the VMware download site.

Procedure

1. Boot an ESXi host that was not provisioned with Auto Deploy.
2. Copy the `/productLocker` directory from the ESXi host to a shared storage.
3. Change the *UserVars.ProductLockerLocation* variable to point to the `/productLocker` directory.
   a. In the vSphere Web Client, select the reference host and click the **Manage** tab.
   b. Select **Settings** and click **Advanced System Settings**.
   c. Filter the settings for **`uservars`**, and select **UserVars.ProductLockerLocation**.
   d. Click the **pen** icon and edit the location so it points to the shared storage.
4. Create a host profile from the reference host.
5. Create an Auto Deploy rule that assigns the `xxxxx-no-tools` image profile and host profile from the reference host to all other hosts.
6. Boot your target hosts with the rule so they pick up the product locker location from the reference host.

Download Auto Deploy Logs

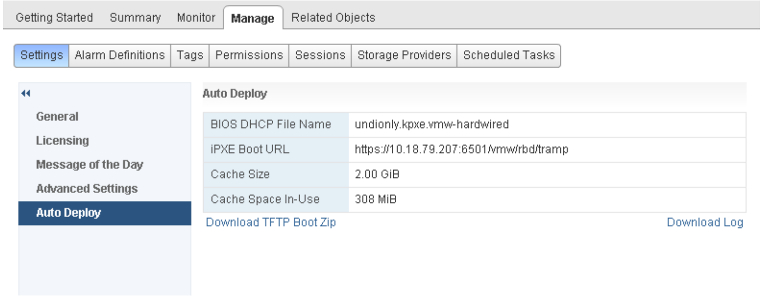
You can use the Auto Deploy logging information from the vSphere Web Client to resolve problems that you encounter with vSphere Auto Deploy.

Prerequisites

Use the vSphere Web Client to log in to the vCenter Server instance that Auto Deploy is registered with.

Procedure

1. Select **vCenter Inventory Lists** and select the vCenter Server system.
2. On the **Manage** tab, select **Settings**, and click **Auto Deploy**.
3. Click **Download Log** to download the log files.



Auto Deploy

BIOS DHCP File Name	undionly.kpxe.vmw-hardwired
iPXE Boot URL	https://10.18.79.207:6501/vmw/rbd/tramp
Cache Size	2.00 GiB
Cache Space In-Use	308 MiB

Troubleshooting Auto Deploy

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

Auto Deploy TFTP Timeout Error at Boot Time

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

Problem

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

Cause

The TFTP server is down or unreachable.

Solution

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

Auto Deploy Host Boots with Wrong Configuration

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

Problem

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

Cause

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

Solution

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

Host Is Not Redirected to Auto Deploy Server

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

Problem

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

Cause

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

Solution

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

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

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

Problem

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

Solution

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

   ESXi Dump Collector is included with the vCenter Server installer.

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

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

3. Use ESXCLI to disable local coredump partitions.

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

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

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

Problem

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

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

Cause

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

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

Solution

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

2 Remove any VIBs that are not stateless-ready.

3 Rerun the Auto Deploy PowerCLI cmdlet.

Auto Deploy Host Reboots After Five Minutes

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

Problem

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

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

The host might also display the following details:

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

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

Cause

No image profile is currently associated with this host.

Solution

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

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

1 Run the `New-DeployRule` cmdlet to create a rule that includes a pattern that matches the host with an image profile.

2 Run the `Add-DeployRule` cmdlet to add the rule to a ruleset.

3 Run the `Test-DeployRuleSetCompliance` cmdlet and use the output of that cmdlet as the input to the `Repair-DeployRuleSetCompliance` cmdlet.

Auto Deploy Host Does Not Network Boot

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

Problem

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

Cause

You did not enable your host for network boot.

Solution

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

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

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

Auto Deploy Host Does Not Get a DHCP Assigned Address

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

Problem

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

Cause

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

Solution

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

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

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

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

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

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

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

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

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

```
netsh firewall set opmode disable
```

   c Attempt to provision the host with Auto Deploy.

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

```
netsh firewall set opmode enable
```

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

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

Auto Deploy Host Cannot Contact TFTP Server

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

Problem

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

Cause

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

Solution

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

Auto Deploy Host Cannot Retrieve ESXi Image from Auto Deploy Server

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

Problem

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

Cause

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

Solution

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

2 Check that the Auto Deploy server is running.

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

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

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

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

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

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

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

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

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

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

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

Recovering from Database Corruption on the Auto Deploy Server

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

Problem

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

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

Cause

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

Solution

1 Stop the Auto Deploy server service.

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

3 Check the logs for the following message:

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

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

4 Go to the Auto Deploy data directory.

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

The directory contains a file named `db`, and backup files named `db-`*yyy-mm-dd*.

5 Rename the current `db` file.

VMware Support might ask for that file if you call for assistance.

6 Rename the most recent backup to `db`.

7 Restart the Auto Deploy server service.

8 If the message still appears in the log, repeat the steps to use the next recent backup until Auto Deploy works without database errors.

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.

Auto Deploy does not support a pure IPv6 environment end-to-end. The PXE boot infrastructure does not support IPv6. After the deployment you can manually reconfigure the hosts to use IPv6 and add them to vCenter Server over IPv6. However, when you reboot a stateless host, its IPv6 configuration is lost.

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.

This proof of concept setup is customized for vCenter Server 6.0 and later. For earlier versions of vCenter Server, go to the corresponding VMware Documentation Center.

For your proof of concept setup, your system must meet specific software and hardware requirements.

Table 4-13. Preinstallation Checklist

Required Software and Hardware	Details
Operating System	A Windows Server 2008 R2 system or later supported Windows system with Microsoft PowerShell preinstalled. For a full list of supported operating systems, see Supported host Operating Systems for VMware vCenter Server installation.
vCenter Server	Version 6.0 or later to be installed on a Windows system. You can also install vSphere PowerCLI on a different Windows system. The Auto Deploy server is part of vCenter Server. You install vSphere PowerCLI on the same Windows system. You perform many of the setup tasks by logging in to that system, either directly into the console or by using Remote Desktop (RDP).
Storage	At least 4 GB of free space on the Windows system where vCenter Server is running. 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 detect the LUNs. ■ A list of target IP addresses for NFS or iSCSI. ■ A list of target volume information for NFS or iSCSI.
Host information (for two or more hosts)	A list of target IP addresses for NFS or iSCSI. A list of target volume information for NFS or iSCSI. ■ Default route, net mask, and primary and secondary DNS server IP addresses. ■ IP address and net mask for the VMkernel primary management network. ■ IP address and net mask for other VMkernel networks such as storage, vSphere FT, or VMware vMotion. Auto Deploy does not overwrite existing partitions by default.
vSphere PowerCLI	vSphere PowerCLI installer binaries downloaded from the Downloads page on the VMware Web site.
ESXi software depot	The location of the ESXi software depot on the Downloads page of the VMware Web site. You use a URL to point to the image profile stored at that location, or you download a ZIP file to work with a local depot. Do not download the ESXi image.
TFTP server	TFTP installer software such as WinAgents TFTP server. The TFTP server included in Windows Server 2008 is closely tied to Windows network deployment and is not suitable.
DHCP server	The DHCP server included with Windows Server 2008 is suitable for this proof of concept setup.

You also need information about and administrator privileges to the environment's core servers including the ActiveDirectory server, DNS server, DHCP server, NTP server, and so on.

You must have complete control of the broadcast domain of the subnet in which you will deploy the setup. Ensure that no other DHCP, DNS, or TFTP server are on this subnet.

Install the TFTP Server

Auto Deploy relies on a TFTP server for sending the boot image to the hosts that it provisions. You must install a TFTP server in your environment.

This task only installs the TFTP server. You later download a configuration file to the server. See "Configure the Auto Deploy and TFTP Environment in the vSphere Web Client," on page 129.

Prerequisites

Make sure your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.

Procedure

1. Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.
2. Download and install the TFTP server software.

   This sample setup uses the TFTP server from WinAgents. The TFTP server that is included with Windows 2008 is closely tied to Windows network deployment and not suitable for Auto Deploy.
3. Configure the TFTP root directory as D:\Drive or a similar location (for example, `D:\TFTP_Root\`).

What to do next

Install and set up vSphere PowerCLI. You use PowerCLI cmdlets to write the rules that assign image profiles and host profiles to hosts. See "Install and Set Up vSphere PowerCLI," on page 126.

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 vSphere PowerCLI on a different Windows system.

Prerequisites

- Verify that Microsoft .NET 4.5 SP2 is installed, or install it from the Microsoft Web site.
- Verify that Windows PowerShell 3.0 is installed, or install it from the Microsoft Web site.

Procedure

1. Log in with administrator privileges to the console of the Windows system on which vCenter Server is installed, either directly or by using RDP.
2. Download vSphere PowerCLI from the Download page of the VMware Web site and install the vSphere PowerCLI software.
3. Confirm that vSphere PowerCLI is working.

   a. Double-click the vSphere PowerCLI icon on the desktop to open a vSphere PowerCLI window.

   b. (Optional) If an SSL error appears, check the thumbprint and ignore the error, and then run `Get-DeployCommand`, and press Enter.

   vSphere PowerCLI displays a list of cmdlets and their definitions in the vSphere PowerCLI window.

What to do next

- If you do not see a list of cmdlets when you run `Get-DeployCommand`, check your vSphere PowerCLI version and uninstall and reinstall it if necessary.

- For some background information on vSphere PowerCLI, see "Using Auto Deploy Cmdlets," on page 85. See the *vSphere PowerCLI User's Guide* for details.
- Prepare the hosts you want to provision with Auto Deploy. See "Prepare Auto Deploy Target Hosts," on page 127.

Prepare Auto Deploy Target Hosts

You must prepare all target hosts for Auto Deploy.

Prerequisites

Hosts that you want to provision with Auto Deploy must meet the requirements for ESXi.

See "ESXi Hardware Requirements," on page 23.

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 127.

Prepare the DHCP Server

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

The proof of concept environment uses Active Directory with DNS and DHCP.

The proof of concept illustrates how to use DHCP reservations. Setting up fixed IP addresses for each host is time consuming and not recommended.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 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 Navigate to **DHCP >** ***hostname*** **> IPv4**.

   c Right-click **IPv4** and select **New Scope**.

   d On the Welcome screen, click **Next**, and specify a name and description for the scope.

   e Specify an IP address range and click **Next**.

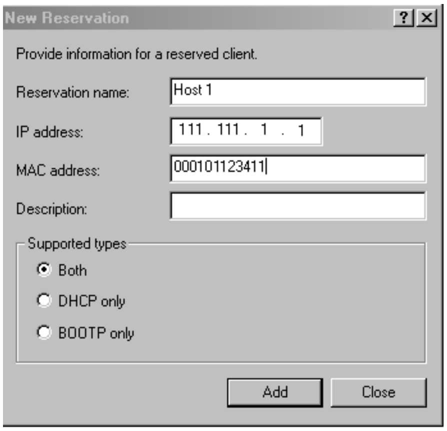
   f Click **Next** until you reach the Configure DHCP Options screen and select **No, I will configure this option later**.

3 If you are planning on using DHCP reservations, create a DHCP reservation for each target ESXi host.

   a In the DHCP window, navigate 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.



Provide information for a reserved client.

Reservation name: Host 1

IP address: 111 . 111 . 1 . 1

MAC address: 000101123411

Description:

Supported types

● Both

○ DHCP only

○ BOOTP only

   d Repeat the process for each of the other hosts.

4 Set up the DHCP Server to point the hosts to the TFTP Server.

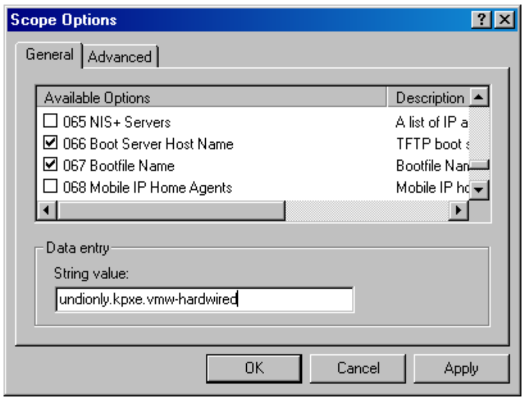
The precise process depends on the DHCP Server you are using. This example uses the DHCP server included with Windows 2008.

   a In the DHCP window, navigate to **DHCP** > ***hostname*** > **IPv4** > **Autodeploy Scope** > **Scope Options**.

   b Right click **Scope Options** and choose **Configure Options**.

   c In the Scope Options window, click the **General** tab.

   d Click **066 Boot Server Host Name** and enter the address of the TFTP server that you installed in the String value field below the Available Options.



Available Options	Description
☐ 065 NIS+ Servers	A list of IP a
☑ 066 Boot Server Host Name	TFTP boot s
☑ 067 Bootfile Name	Bootfile Nan
☐ 068 Mobile IP Home Agents	Mobile IP hc

Data entry

String value: undionly.kpxe.vmw-hardwired

   e Click **067 Bootfile Name** and enter **`undionly.kpxe.vmw-hardwired`**.

   The `undionly.kpxe.vmw-hardwired` iPXE binary will be used to boot the ESXi hosts.

   f Click **Apply** and click **OK** to close the window.

5 In the DHCP window, right-click **DHCP** > ***hostname*** > **IPv4** > **Scope** > **Activate** and click **Activate**.

6 Do not log out from the DHCP Server if you are using Active Directory for DHCP and DNS, or log out otherwise.

What to do next

Prepare the DNS Server. See "Prepare the DNS Server," on page 129.

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 124 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.

Configure the Auto Deploy and TFTP Environment in the vSphere Web Client

You must download a TFTP Boot ZIP file from your Auto Deploy server. The customized FTP server serves the boot images that Auto Deploy provides. You can perform the task in the vSphere Web Client.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.

Procedure

1 From your Web browser, access the URL of the vSphere Web Client that connects to the vCenter Server system that manages the Auto Deploy server.

2 When the Certificate warning appears, continue to the vCenter Server system.

3 Start the Auto Deploy service.

a On the vSphere Web Client Home page, click **Administration**.

b Under **System Configuration** click **Services**.

c Select **Auto Deploy**, click the **Actions** menu, and select **Start**.

On Windows, the Auto deploy service can be disabled. You can enable the service by changing the Auto Deploy service startup type.

4 In the inventory, navigate to the vCenter Server system.

5 On the Manage tab, select **Settings**, and click **Auto Deploy**.

6 Click the **Download TFTP Boot Zip** link to download the TFTP configuration file.

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.

8 Minimize the Web browser you are using with the vSphere Web Client.

What to do next

Prepare the depot from which Auto Deploy retrieves the ESXi software when it provisions the hosts. See "Prepare the ESXi Software Depot," on page 130.

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

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 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-N.N.N-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-version-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 131.

Set Up the First Host and Provision with Auto Deploy

Setting up the first host requires that you understand how to write Auto Deploy rules with vSphere PowerCLI. After you write the rules and add them to the ruleset, you can turn on the host to provision it.

You use the PowerCLI command-line interface to specify how Auto Deploy provisions the target hosts. You define rules and add each rule to the active ruleset. The Auto Deploy server checks the ruleset to determine which image profile to send to each ESXi host, which host profile to send to each ESXi host, and which location on the vCenter Server to place the host in.

A rule allows you to specify the following parameters.

Parameter	Description
Name	Name of the rule, specified with the `-Name` parameter.
Item	One or more items, specified with the `-Item` parameter. An item can be an image profile to be used, a host profile to be used, or a vCenter Server inventory location (datacenter, folder, cluster) for the target host. You can specify multiple items separated by commas.
Pattern	The pattern specifies the host or group of hosts to which the rule applies. Choose one of the following. **vendor** Machine vendor name. **model** Machine model name. **serial** Machine serial number. **hostname** Machine hostname. **domain** Domain name. **ipv4** IPv4 address of the machine. **mac** Boot NIC MAC address. **asset** Machine asset tag. **oemstring** OEM-specific strings in the SMBIOS. Specify `-AllHosts` to apply the item or items to all hosts.

This proof of concept setup first uses `-AllHosts` and later uses an IP address range to identify the hosts to provision.

Write Rules for the First Host

You specify the image profile to provision the host with by using PowerCLI to write a rule and adding the rule to the active ruleset.

This task assumes you have a basic knowledge of Microsoft PowerShell and vSphere PowerCLI.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.

- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.
- Make sure you can access the ESXi software from the system on which you run the PowerCLI cmdlets.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

  This task assumes that you installed PowerCLI on the system on which the vCenter Server system is running.

2 Open the PowerCLI window and list the ESXi image profiles.

```
Get-EsxImageProfile
```

3 Create a new rule by running the following cmdlet, replacing ESXi-5.1.0-*XXXXX*-standard with the image profile that you want to use.

```
New-DeployRule -Name "InitialBootRule" -Item "Esxi-5.1.0-XXXXX-standard" -AllHosts
```

4 Add the new rule to the active rule set to make the rule available to the Auto Deploy server.

```
Add-DeployRule -DeployRule "InitialBootRule"
```

What to do next

Boot the host and check that Auto Deploy provisions the host and adds it to the vCenter Server inventory. See "Provision the First Host," on page 132.

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

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.

Procedure

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

  During the boot process, DHCP assigns an IP address to the host. The IP address matches a name you specified earlier in the DNS server. The host contacts the Auto Deploy server and downloads the ESXi binaries from the HTTP URL indicated in the iPXE tramp file that you downloaded into the TFTP_Root directory earlier. Each instance of Auto Deploy produces a custom set of files for the TFTP Server.

2 With a vSphere Web Client and connect to the vCenter Server system.

  In this proof of concept setup, the vCenter Server system is localhost.

3 Click **Hosts and Clusters**.

4 Check that the newly provisioned host is now in the vCenter Server inventory at the datacenter level.

  By default, Auto Deploy adds hosts at the datacenter level when the boot process completes.

What to do next

If you encounter problems, see "Troubleshooting Auto Deploy," on page 118.

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 133.

Configure the Proof of Concept Reference Host

You can customize the first ESXi host that you boot for your environment and create a host profile. You can set up Auto Deploy to provision other target hosts with that host profile. The ESXi host you create the host profile from is considered your reference host or template host.

How you configure the reference host depends on what you want to do.

Shared settings

Specify settings that all hosts share and save a host profile for the host.

Host-specific settings

Customize hosts by setting up the host profile to prompt for user input for a limited number of options such as a static IP address. Host customizations are saved when you save the host profile. See "Host Customization in the vSphere Web Client," on page 109.

Auto Deploy applies all common settings from the host profile to all target hosts. If you set up the host profile to ask for user input, all hosts provisioned with that host profile come up in maintenance mode. You must reapply the host profile or reset host customizations to be prompted for the host-specific information.

NOTE Administrators cannot directly access or manipulate host customizations. Use the vSphere Web Client Host Profiles UI to work with host customizations.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.

Procedure

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

   In this proof of concept setup, the vCenter Server system is localhost.

2. Click Hosts and Clusters and select the host that Auto Deploy added to the first datacenter.

3. Configure the host.

   The rest of the proof of concept setup assumes that you configure at least one setting that is different for different hosts.

Configuration	Description
Networking	Configure the following networking components. ■ Base virtual switch and management port group for VMkernel. ■ Storage network port group for VMkernel. ■ Virtual machine networking port group. ■ Any additional virtual switches and port groups. ■ Distributed switches, if necessary (transfer port groups to distributed switches if you use them).
Storage	Configure shared storage.
Time settings	Configure your time settings.
Security	Configure the security profile.
Authentication	Configure authentication.

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 the *Host Profiles* documentation.

Create and Apply a Host Profile with the vSphere Web Client

Configuration that is shared by a group of hosts is stored in a host profile. You can create the host profile from your reference host. Configuration that differs for different hosts, such as a static IP address, can be managed through the host customization mechanism.

Auto Deploy can provision each host with the same host profile. In certain cases, Auto Deploy also uses host customizations that allow you to specify information that differs for different hosts. For example, if you set up a VMkernel port for vMotion or for storage, you can specify a static IP address for the port by using the host customization mechanism.

In this example, you extract a host profile from a reference host, attach the host profile to one other host, and check host profile compliance. In most cases, you do not perform these tasks manually but you write an Auto Deploy rule that applies a host profile to hosts that are provisioned with Auto Deploy. See "Write a Rule and Assign a Host Profile to Hosts," on page 88.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.

Procedure

1. Log in to a vSphere Web Client that is connected to the vCenter Server system with administrator privileges.
2. Click **Rules and Profiles** and select **Host Profiles**.
3. Click the Extract profile from host icon and respond to the wizard prompts.

Option	Description
Select Host	Select the reference host you configured earlier.
Name and Description	Name the profile ESXiGold and add a description.
Ready to Complete	Review the information and click **Finish**.

4. Right-click the ESXiGold host profile, select **Attach/Detach Hosts and Clusters**.
5. Select the ESXi host to which you want to attach the profile, click **Attach**, and click **Next**.

   The wizard loads the host customization.
6. Provide any customization information and click **Finish**.

What to do next

Create a rule that assigns the image profile and the newly-created host profile to all hosts you want to provision with Auto Deploy. See "Create a Rule for Other Target Hosts," on page 135.

Create a Rule for Other Target Hosts

You can create a rule that applies the previously verified image profile and the host profile that you just created to all target hosts.

This task assumes you have a basic knowledge of Microsoft PowerShell and vSphere PowerCLI.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 for the complete list.

Procedure

1 Log in to the console of the Windows system on which vCenter Server is installed with administrator privileges, either directly or by using RDP.

2 Start a PowerCLI session and type the following commands, followed by Enter, at the prompt.

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

Include the complete path and file name of the ZIP file you downloaded earlier. Adding the software depot is required each time you start a new PowerCLI session.

3 (Optional) To display the rules in the active ruleset type he following cmdlet at the prompt and press Enter.

```
Get-DeployRuleset
```

4 To create a rule that instructs Auto Deploy to provision the set of hosts in the specified IP range with the image you selected and with the host profile you created from the reference host, type the following command and press Enter.

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

Option	Description
image_profile	The ESXi image profile you used in the first deploy rule.
target_cluster	Name of the cluster in vCenter Server to which you want to add all hosts.
IP_range	Either a single IP address or a range of IP addresses for the hosts you want to provision with the image profile and host profile.

When you specify a target cluster, the host profile is applied to all hosts in the cluster. Applying the host profile to each host is not required.

5 Add the new rule to the active ruleset.

`Add-DeployRule -DeployRule "Production01Rule"` <Enter>

6 (Optional) Remove the deploy rule you created for the initial boot operation.

`Remove-DeployRule -DeployRule InitialBootRule` <Enter>

7 Check the active rule set.

`Get-DeployRuleset`<Enter>

PowerCLI displays information similar to the following example.

```
Name:              Production01Rule
PatternList:       {ipv4=address_range}
ItemList:          {ESXi-version-XXXXXX-standard, Compute01, ESXiGold}
```

What to do next

Provision all hosts and set up host customizations for each host. See "Provision All Hosts and Set Up Host Customizations," on page 136.

Provision All Hosts and Set Up Host Customizations

With the rule in place that provisions hosts using an image profile, and with the host profile created from the reference host available, you can provision all target hosts. If any host profile items are set to prompt the user for input, the host comes up in maintenance mode. You apply the host profile or check host compliance to be prompted for the information. The system associates the host customization with the host.

Prerequisites

- Verify that your system meets the requirements in the preinstallation checklist. See "Proof of Concept Preinstallation Checklist," on page 124.
- Perform all preceding proof of concept setup tasks. See "Auto Deploy Proof of Concept Setup," on page 124 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 With a vSphere Web Client, connect to the vCenter Server system.

3 Click **Home** and select **Host Profiles**.

4 In the panel on the left, select the ESXiGold profile and add the newly booted hosts to that profile.

5 Apply the host profile to each of the hosts, provide the user input information, and reboot each host.

When the reboot progress completes, all hosts are running with the image you specify and use the configuration in the reference host profile. The cluster shows that all hosts are fully compliant.

All hosts are now configured with the shared information through the reference host profile and with the host-specific information through the host customization mechanism. The next time you boot the hosts, they retrieve that information and boot completely.

What to do next

With your proof of concept implementation completed successfully, you can start planning your production setup.

Using vSphere ESXi Image Builder

vSphere ESXi Image Builder is a set of vSphere 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 vSphere ESXi 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.

Understanding vSphere ESXi Image Builder

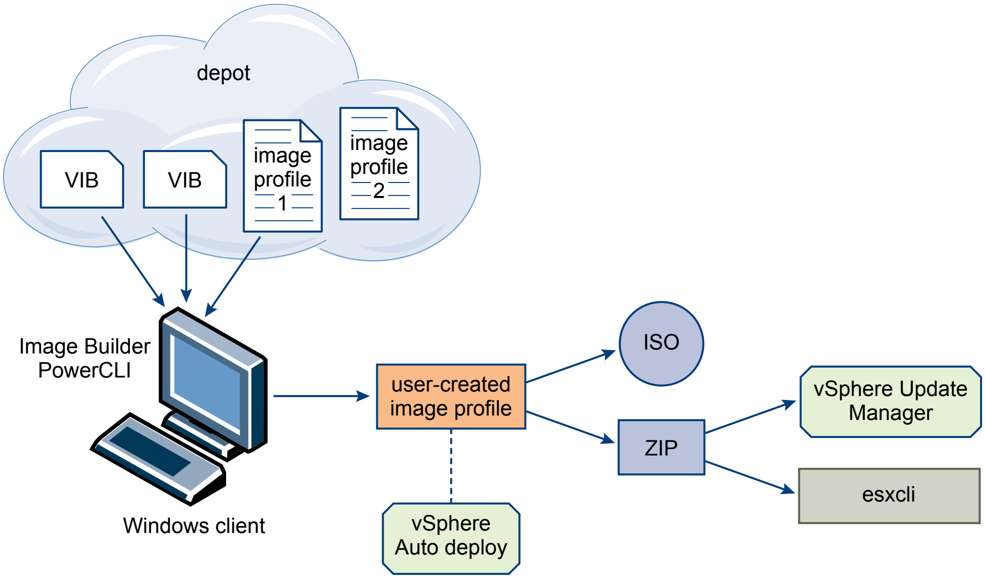
You can use the VMware vSphere® ESXi™ Image Builder CLI to manage software depots, image profiles, and software packages (VIBs). Image profiles and VIBs specify the software you want to use during installation or upgrade of an ESXi host.

vSphere ESXi Image Builder Overview

vSphere ESXi Image Builder lets you manage vSphere image profiles and VIBs.

VIBs are software packages, and image profiles contain a set of software packages. See "Software Depots and Their Components," on page 138.

Figure 4-6. Image Builder Architecture



You use vSphere ESXi Image Builder cmdlets for managing the software to deploy to your ESXi hosts in several different situations.

Table 4-14. Cases Where You Can Use vSphere ESXi Image Builder

Use Case for vSphere ESXi Image Builder	Description
Create image profiles for use by vSphere Auto Deploy	Use vSphere ESXi Image Builder to create an image profile that defines the VIBs that vSphere Auto Deploy uses to provision hosts.
Add custom third-party drivers to existing image profile and export to ISO or bundle	When you add third-party driver or extension custom VIBs to your ESXi hosts, use vSphere ESXi Image Builder to clone the base image provided by VMware, add the custom VIBs, and export to ISO or to offline bundle ZIP file.

Table 4-14. Cases Where You Can Use vSphere ESXi Image Builder (Continued)

Use Case for vSphere ESXi Image Builder	Description
Perform upgrades	If you upgrade from a 4.0 or 4.1 system that includes custom extensions or drivers, you can use vSphere ESXi Image Builder to create an image profile that includes the vSphere 5 base VIB. You can create vSphere 5 VIBs for the custom extensions and add those VIBs to the base VIB. Export the custom image profile to an ISO you can install or to a ZIP that you can use with vSphere Update Manager.
Create custom images with reduced footprint	If you require a minimal footprint image, you can clone the ESXi base image profile and remove VIBs using vSphere ESXi Image Builder.

The vSphere ESXi Image Builder cmdlets take image profiles and VIBs as input and produce various outputs.

Table 4-15. Input and Output to the vSphere ESXi Image Builder Cmdlets

Parameter	Description
Input	Image profiles and VIBs that are located in a software depot are used as input to vSphere PowerCLI cmdlets running on a Windows client.
Output	vSphere PowerCLI cmdlets create custom image profiles that can be exported to an ISO image or an offline depot ZIP file. ISO images are used for installation. The ZIP depot can be used by Update Manager or by `esxcli software` commands to update or install images. Image profiles are also used in vSphere Auto Deploy rules to customize the software to provision ESXi hosts with.

Watch the video "Using Image Builder CLI" for information about vSphere ESXi Image Builder:

Using Image Builder CLI (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_using_image_builder_cli)

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 142.

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 by using vSphere ESXi Image Builder.

See "ImageProfile Object Properties," on page 141.

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.

vSphere ESXi Image Builder Cmdlets Overview

vSphere ESXi Image Builder cmdlets allow you to manage image profiles and VIBs.

vSphere ESXi Image Builder includes the following cmdlets.

Note When you run vSphere ESXi 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 vSphere PowerCLI prompt for detailed reference information.

Table 4-16. vSphere ESXi Image Builder Cmdlets

Cmdlet	Description
`Add-EsxSoftwareDepot`	Adds the software depot or ZIP file at the specified location to your current environment. Downloads metadata from the depot and analyzes VIBs for dependencies.
`Remove-EsxSoftwareDepot`	Disconnects from the specified software depot.
`Get-EsxSoftwareDepot`	Returns a list of software depots that are in the current environment. If you want to examine and manage image profiles and VIBs, you must first add the corresponding software depot to your environment.
`Get-EsxSoftwarePackage`	Returns a list of software package objects (VIBs). Use this cmdlet's options to filter the results.
`Get-EsxImageProfile`	Returns an array of `ImageProfile` objects from all currently added depots.
`New-EsxImageProfile`	Creates a new image profile. In most cases, creating a new profile by cloning an existing profile is recommended. See "Clone an Image Profile," on page 146.
`Set-EsxImageProfile`	Modifies a local `ImageProfile` object and performs validation tests on the modified profile. The cmdlet returns the modified object but does not persist it.
`Export-EsxImageProfile`	Exports an image profile as either an ESXi ISO image for ESXi installation, or as a ZIP file.
`Compare-EsxImageProfile`	Returns an `ImageProfileDiff` structure that shows whether the two profiles have the same VIB list and acceptance level. See "Acceptance Levels," on page 141.
`Remove-EsxImageProfile`	Removes the image profile from the software depot.
`Add-EsxSoftwarePackage`	Adds one or more new packages (VIBs) to an existing image profile.
`Remove-EsxSoftwarePackage`	Removes one or more packages (VIBs) from an image profile.

Image Profiles

Image profiles define the set of VIBs that an ESXi installation or update process uses. Image profiles apply to hosts provisioned with vSphere Auto Deploy and to other ESXi 5.x hosts. You define and manipulate image profiles with vSphere ESXi Image Builder.

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 vSphere ESXi Image Builder 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, vSphere ESXi Image Builder checks that the change does not invalidate the profile.

Dependency Validation

When you add or remove a VIB, vSphere ESXi 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 141

Acceptance Level Validation

vSphere ESXi Image Builder performs acceptance level validation each time an image profile is created or changed. vSphere ESXi 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, vSphere ESXi 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 vSphere Auto Deploy server uses VIBs.
- Checks that VIBs follow file path usage rules. VMware tests VMwareCertified and VMwareAccepted VIBs to guarantee those VIBs always follow file path usage rules.

Acceptance Levels

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host. You can change the host acceptance levels with `esxcli` commands.

VMware supports the following acceptance levels.

VMwareCertified
The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only IOVP drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.

VMwareAccepted
VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins 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 CommunitySupported 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

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` vSphere PowerCLI cmdlet, has the following properties.

Name	Type	Description
`AcceptanceLevel`	`AcceptanceLevel`	Determines which VIBs you can add to the profile. Levels are VMwareCertified, VMwareAccepted, PartnerSupported, and CommunitySupported. See "Acceptance Levels," on page 141.
`Author`	`System.String`	The person who created the profile. 60 characters or fewer.

Name	Type	Description
CreationTime	System.DateTime	The timestamp of creation time.
Description	System.String	The full text description of profile. No length limit.
GUID	System.String	Globally unique ID of the image profile.
ModifiedTime	System.DateTime	The timestamp of last modification time.
Name	System.String	The name of the image profile. 80 characters or fewer.
ReadOnly	System.Boolean	When set to true, the profile cannot be edited. Use Set-EsxImageProfile -Readonly to make your custom image profiles read-only.
Rules	ImageProfileRule[]	Any OEM hardware requirements and restrictions that the image profile might have. vSphere Auto Deploy verifies the value of this property when deploying an image profile and deploys the profile if matching hardware is available.
Vendor	System.String	The organization that publishes the profile. 40 characters or fewer.
VibList	SoftwarePackage[]	The list of VIB IDs the image contains.

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	The acceptance level of this VIB.
Conflicts	SoftwareConstraint[]	A list of VIBs that cannot be installed at the same time as this VIB. Each constraint uses the following format: package-name[<<|<=|=|>=|<< version]
Depends	SoftwareConstraint[]	A list of VIBs that must be installed at the same time as this VIB. Same constraint format as Conflicts property.
Description	System.String	The long description of the VIB.
Guid	System.String	The 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.
MaintenanceMode	System.Boolean	True if hosts must be in maintenance mode for installation of this VIB.
Name	System.String	The name of the VIB. Usually uniquely describes the package on a running ESXi system.

Name	Type	Description
`Provides`	`SoftwareProvides`	The list of virtual packages or interfaces this VIB provides. See "SoftwareProvide Object Properties," on page 145.
`ReferenceURLs`	`SupportReference[]`	The list of `SupportReference` objects with in-depth support information. The `SupportReference` object has two properties, `Title` and `URL`, both of type `System.String`.
`Replaces`	`SoftwareConstraint[]`	The list of `SoftwareConstraint` objects that identify VIBs that replace this VIB or make it obsolete. VIBs automatically replace VIBs with the same name but lower versions.
`ReleaseDate`	`System.DateTime`	Date and time of VIB publication or release.
`SourceUrls`	`System.String[]`	The list of source URLs from which this VIB can be downloaded.
`StatelessReady`	`System.Boolean`	True if the package supports host profiles or other technologies that make it suitable for use in conjunction with vSphere Auto Deploy.
`Summary`	`System.String`	A one-line summary of the VIB.
`Tags`	`System.String[]`	An array of string tags for this package defined by the vendor or publisher. Tags can be used to identify characteristics of a package.
`Vendor`	`System.String`	The VIB vendor or publisher.
`Version`	`System.String`	The VIB version.
`VersionObject`	`Software.Version`	The `VersionObject` property is of type `SoftwareVersion`. The `SoftwareVersion` class implements a static `Compare` method to compare two versions of strings. See "SoftwareVersion Object Properties," on page 144

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`	The acceptance level for the second profile that you passed to `Compare-EsxImageProfile`.
`DowngradeFromRef`	`System.String[]`	The 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.

Name	Type	Description
OnlyInComp	System.String	The list of VIBs found only in the second profile that you passed to Compare-EsxImageProfile.
OnlyInRef	System.String[]	The list of VIBs found only in the first profile that you passed to Compare-EsxImageProfile.
PackagesEqual	System.Boolean	True if the image profiles have identical sets of VIB packages.
RefAcceptanceLevel	System.String	The acceptance level for the first profile that you passed to Compare-EsxImageProfile.
UpgradeFromRef	System.String[]	The list of VIBs in the second profile that are upgrades from VIBs in the first profile.

SoftwareVersion Object Properties

The SoftwareVersion object lets you compare two version strings. The object includes a Comparestatic method that accepts two strings as input and returns 1 if the first version string is a higher number than the second version string. Compare returns 0 if two versions strings are equal. Compare returns -1 if the second version string is a higher number than the first string. The object has the following properties.

Name	Type	Description
Version	System.String	The part of the version before the hyphen. This part indicates the primary version.
Release	System.String	The part of the version after the hyphen. This part indicates the release version.

SoftwareConstraint Object Properties

The SoftwareConstraint object implements a MatchesProvide method. The method accepts a SoftwareProvides or SoftwarePackage object as input and returns True if the constraint matches the SoftwareProvide or the SoftwarePackage, or returns False otherwise.

The SoftwareConstraint object includes the following properties.

Name	Type	Description
Name	System.String	The name of the constraint. This name should match a corresponding SoftwareProvide Name property.
Relation	System.String	An enum, or one of the following comparison indicators: <<, <=, = >=, >>. This property can be $null if the constraint does not have a Relation and Version property.
Version	System.String	The version to match the constraint against. This property can be $null if the constraint does not have a Relation and Version property.
VersionObject	SoftwareVersion	The version represented by a SoftwareVersion object.

SoftwareProvide Object Properties

The `SoftwareProvide` object includes the following properties.

Name	Type	Description
`Name`	`System.String`	The name of the provide.
`Version`	`System.String`	The version of the provide. Can be $null if the provide does not specify a version.
`Release`	`System.String`	The version of the provide as represented by a SoftwareVersion object. See "SoftwareVersion Object Properties," on page 144.

vSphere ESXi Image Builder Installation and Usage

vSphere ESXi Image Builder consists of the vSphere ESXi Image Builder server and the vSphere ESXi Image Builder PowerShell cmdlets. The vSphere ESXi Image Builder server starts when your run the first vSphere ESXi Image Builder cmdlet.

Install vSphere ESXi Image Builder and Prerequisite Software

Before you can run vSphere ESXi Image Builder cmdlets, you must install vSphere PowerCLI and all prerequisite software. The vSphere ESXi Image Builder snap-in is included with the vSphere PowerCLI installation.

You install vSphere ESXi Image Builder and prerequisite software on a Microsoft Windows system.

Procedure

1. Install Microsoft .NET 2.0 from the Microsoft website following the instructions on that website.
2. Install Microsoft PowerShell 2.0. from the Microsoft website following the instructions on that website.
3. Install vSphere PowerCLI, which includes the vSphere ESXi Image Builder cmdlets.

   See the *vSphere PowerCLI Installation Guide* for detailed instructions.

What to do next

Review "Using vSphere ESXi Image Builder Cmdlets," on page 145.If you are new to vSphere PowerCLI, read the vSphere PowerCLI documentation.

Use vSphere ESXi Image Builder cmdlets and other vSphere PowerCLI cmdlets and PowerShell cmdlets to manage image profiles and VIBs. Use `Get-Help` *cmdlet_name* at any time for command-line help.

Using vSphere ESXi Image Builder Cmdlets

vSphere ESXi Image Builder cmdlets are implemented as Microsoft PowerShell cmdlets and included in vSphere PowerCLI. Users of vSphere ESXi Image Builder cmdlets can take advantage of all vSphere PowerCLI features.

Experienced PowerShell users can use vSphere ESXi Image Builder cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and vSphere PowerCLI, follow these tips.

You can type cmdlets, parameters, and parameter values in the vSphere 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`.
- Use wildcards for searching and filtering VIBs and image profiles. All wildcard expressions are supported.

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 of the examples in the *vSphere Installation and Setup* documentation pass in parameters by name. "vSphere ESXi Image Builder Workflows," on page 155 includes examples that pass parameters as objects.

vSphere ESXi Image Builder Common Tasks

The vSphere ESXi Image Builder cmdlets allow you to manipulate software depots, image profiles, and VIBs.

Clone 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 new profile.

Prerequisites

- Install the vSphere PowerCLI and all prerequisite software. See "vSphere ESXi Image Builder Installation and Usage," on page 145.
- Verify that you have access to the software depot that contains the image profile you want to clone.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2 (Optional) Run the `Get-EsxImageProfile` cmdlet to find the name of the profile that you want to clone.

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 "Examine Depot Contents," on page 155 for some examples of filtering.

Customize the image profile by adding or removing VIBs. See "Add VIBs to an Image Profile," on page 147.

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 read only. 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, vSphere ESXi Image Builder performs validation. If you add VIBs from two or more OEM partners simultaneously, no errors are reported but the resulting image profile might not work. Install VIBs from only one OEM vendor at a time.

If an error about acceptance level problems appears, change the acceptance level of the image profile and the acceptance level of the host. Consider carefully whether changing the host acceptance level is appropriate. VIB acceptance levels are set during VIB creation and cannot be changed.

You can add VIBs even if the resulting image profile is invalid.

Note VMware can support only environments and configurations that are proven to be stable and fully functional through rigorous and extensive testing. Use only those supported configurations. You can use custom VIBs if you lower your host acceptance level, and as a result, supportability. In that case, track the changes you made, so you can revert them if you want to remove custom VIBs and restore the host acceptance level to the default (Partner Supporter) later. See "Working with Acceptance Levels," on page 152.

Prerequisites

Install the vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2 Run the `Get-EsxImageProfile` cmdlet to list all image profiles in all currently visible depots.

The cmdlet returns all available profiles. You can narrow your search by using the optional arguments to filter the output.

3 Clone the profile.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
```

Image profiles published by VMware and its partners are read only. To make changes, you must clone the image profile. The `vendor` parameter is required.

4 Run the `Add-EsxSoftwarePackage` cmdlet to add a new package to one of the image profiles.

```
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 occurs.

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.

Prerequisites

Install the vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

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

Export Format	Cmdlet
ISO images	`Export-EsxImageProfile` with the `-ExportToIso` parameter
Offline depot ZIP files	`Export-EsxImageProfile` with the `-ExportToBundle` parameter

For the ISO image, vSphere ESXi Image Builder validates VIB signatures, adds VIB binaries to the image, and downloads the image to the specified location. For the ZIP file, vSphere ESXi Image Builder validates VIB signatures and downloads the VIB binaries to the specified location.

Example: Exporting an Image Profile to ISO

Example: Exporting an Image Profile to Offline Bundle

Follow these steps to export an image profile to an ISO image or a ZIP file of component files and folders.

1 Add the software depot.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 View 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
```

1 Add the software depot.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 View 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 vSphereUpdate 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 vSphere 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 vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, create an image profile, for example by cloning an existing image profile and adding a VIB.

2 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 vSphere PowerCLI session.

4 When you start a new vSphere PowerCLI session, add the depot that contains your image profile to access it.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Compare Image Profiles

You can compare two image profiles by using the Compare-EsxImageProfile cmdlet, for example, to see if they have the same VIB list or acceptance level . Comparing image profiles or their properties is also possible by using the PowerShell comparison operators.

Prerequisites

Install the vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, run the Add-EsxSoftwareDepot cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run Add-EsxSoftwareDepot -DepotUrl *depot_url*.
ZIP file	a Download the ZIP file to a local file system. b Run Add-EsxSoftwareDepot -DepotUrl C:\file_path\*offline-bundle*.zip

The cmdlet returns one or more SoftwareDepot objects.

2 (Optional) Run the Get-EsxImageProfile cmdlet to view a list of all image profiles in all available depots.

In the list, you can locate the names of the image profiles you want to compare.

3 Before comparing the image profiles, assign them to variables.

For example, you can create variables $imageProfile1 and $imageProfile2 to hold the names of the compared images profiles.

```
$imageProfile1
               = Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
               = Get-EsxImageProfile -Name "ImageProfile2"
```

4 Compare the two image profiles by using the `Compare-EsxImageProfile` cmdlet or the `-eq` comparison operator, which returns a Boolean value.

- Compare the two image profiles to get a full description of the differences by using the `Compare-EsxImageProfile` cmdlet.

  ```
  Compare-EsxImageProfile -ReferenceProfile
                       $imageProfile1 -ComparisonProfile $imageProfile2
  ```

- Compare the two image profiles by VIB list and acceptance level using the `-eq` comparison operator.

  ```
     if ($imageProfile1 -eq $imageProfile2) {
        Write-host "Successfully verified that both image profiles are equal."
     } else {
        Write-host "Failed to verify that the image profiles are equal."
     }
  ```

- Compare the two image profiles by a specific property using the `-eq` comparison operator.

  ```
     if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
        Write-host "Successfully verified that both image profiles are equal."
     } else {
        Write-host "Failed to verify that the image profiles are equal."
     }
  ```

Compare VIBs

You can compare two VIBs or their properties by using the PowerShell comparison operators.

Prerequisites

Install the vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2 (Optional) Run the `Get-EsxSoftwarePackage` cmdlet to view all available VIBs.

In the list, you can locate the names of the VIBs you want to compare.

3 Before comparing the VIBs, assign them to variables.

For example, you can create variables `$vib1` and `$vib2` to hold the names of the compared VIBs.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

4 Use a comparison operator to compare the VIBs by contents and acceptance level or by a specific property.

- Compare the two VIBs by their contents and acceptance level.

  ```
  if ($vib1 -eq $vib2) {
     Write-host "Successfully verified that both VIBs are equal."
  } else {
     Write-host "Failed to verify that the VIBs are equal."
  }
  ```

- Compare a specific property of the VIBs by using a comparison operator such as `-eq`, `-lt`, `-le`, `-gt` or `-ge`.

  ```
  if ($vib1.VersionObject -lt $vib2.VersionObject) {
     Write-host "Successfully verified that both the VIBs are equal."
  } else {
     Write-host "Failed to verify that the VIBs are equal."
  }
  ```

Working with Acceptance Levels

Hosts, image profiles, and individual VIBs have acceptance levels. VIB acceptance levels show how the VIB was tested. 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, contact your 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 154.

The vSphere Update Manager does not display the actual acceptance level. Use vSphere ESXi Image Builder 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 occurs. Change the acceptance level of the host to install the image profile or VIB. See "Change the Host Acceptance Level," on page 153. Changing the acceptance level of the host changes the support level for that host.

The acceptance level of a host, image profile, or VIB lets you 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 plug-ins 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 CommunitySupported 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 acceptance level of the host. 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. For more information on acceptance levels, see "Acceptance Levels," on page 141.

Changing the host acceptance level to CommunitySupported affects the supportability of your host and might affect the security of your 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
View information for all VIBs	`esxcli --server=server_name software sources vib list --depot=depot_URL`
View information for a specified VIB	`esxcli --server=server_name software sources vib list --viburl=vib_URL`

Option	Description
View information for all image profiles	`esxcli --server=`*server_name* `software sources profile list --depot=`*depot_URL*
View information for a specified image profile	`esxcli --server=`*server_name* `software sources profile get --depot=`*depot_URL* `--profile=`*profile_name*

2 View the host acceptance level.

```
esxcli --server=server_name software acceptance get
```

3 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 you enforce a VIB or image profile with lower acceptance level than the acceptance level of the host and your setup is no longer consistent. The warning is repeated when you install VIBs, remove VIBs, or 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 acceptance level of the VIB is lower than that of the image profile, you can clone the image profile with a lower acceptance level or change the image profile's acceptance level.

You can specify VMwareCertified, VMwareAccepted, PartnerSupported, or CommunitySupported as an acceptance level of an image profile. If you lower the acceptance level, the level of support for the image profile and hosts that you provision with it changes. For more information, see "Acceptance Levels," on page 141.

Prerequisites

Install vSphere PowerCLI and all prerequisite software. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

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
```

vSphere ESXi Image Builder Workflows

vSphere ESXi 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 vSphere PowerCLI, Microsoft PowerShell, or both.

Examine Depot Contents

You can examine software depots and VIBs with vSphere ESXi Image Builder cmdlets. You can use wildcards to examine depot contents. All wildcard expressions are supported.

The workflow itself passes parameters by name. However, you can pass parameters as objects by accessing variables.

You can use filtering options and wildcard expressions to examine depot contents.

Prerequisites

Verify that vSphere PowerCLI and prerequisite software is installed. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

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 created by a vendor with a name that starts with the letter C.

3 Retrieve software packages by using the `Get-EsxSoftwarePackage` cmdlet.

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 the letter V.

- `Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"`

  Returns all software packages with a name that contains the string `scsi` in it from a vendor with a name that starts with the letter V.

- `Get-EsxSoftwarePackage -Version "2.0*"`

  Returns all software packages with a version string that starts with 2.0.

4 Use -Newest to find the latest package.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest`

     Returns the newest package for the vendors with a name that starts with the letter V, and displays the information as a table.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list`

     Returns detailed information about each software package by using a pipeline to link the output of the request for software packages to the PowerShell format-list cmdlet.

5 View the list of VIBs in the image profile.

```
(Get-EsxImageProfile -Name "Robin's Profile").VibList
```

VibList is a property of the ImageProfile object.

6 Retrieve software packages released before or after a certain date by using the CreatedBefore or CreatedAfter parameter.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Example: Depot Content Examination Using Variables

This workflow example 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 vSphere PowerCLI prompt. Replace names with names that are appropriate in your installation.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Create Image Profiles by Cloning Workflow

You can use vSphere ESXi Image Builder cmdlets to check which depots are available, to add a depot, to view image profile information, and to create a new image profile by cloning one of the available image profiles.

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.

Prerequisites

Verify that vSphere PowerCLI and prerequisite software is installed. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

Procedure

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 the depot containing the profile that you want to clone does not appear in the results, add it to the current session.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
ZIP file	a Download the ZIP file to a local file path. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`

PowerShell adds the specified depot to your current session and lists all current depots.

3 (Optional) Check the `$DefaultSoftwareDepots` variable, which now returns the newly added depot.

4 View all available image profiles.

```
Get-EsxImageProfile
```

5 To clone an image profile, enter its name, a new name for the new profile, and a name of the vendor.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor
"Vendor20"
```

6 (Optional) View the newly created image profile, `$ip`.

PowerShell returns the information about the image profile in tabular format.

```
Name              Vendor          Last Modified          Acceptance Level
----              ------          -------------          ----------------
Test Profile 42   Vendor20        9/15/2010 5:45:43...   PartnerSupported
```

Example: Creating Image Profile by Cloning Using Variables

This workflow example repeats the steps of this workflow by passing in parameters as objects accessed by position in a variable, instead of passing in parameters by name. You can run the following cmdlets in sequence from the vSphere PowerCLI prompt.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Create New Image Profiles Workflow

In most situations, you create an image profile by cloning an existing profile. Some VMware customers or partners might need to create a new image profile. Pay careful attention to dependencies and acceptance levels if you create an image profile from scratch.

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. If you have to add a VIB with a lower acceptance level to the image profile, you must lower the image profile acceptance level. For more information, see "Set the Image Profile Acceptance Level," on page 154.

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.

Prerequisites

- vSphere PowerCLI and prerequisite software is installed. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.

- You have access to a depot that includes a base image and one or more VIBs. VMware and VMware partners have public depots, accessible by a URL. VMware or VMware partners can create a ZIP file that you can unzip to your local environment and access by using a file path.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2 Run the `Get-EsxImageProfile` cmdlet to list all image profiles in all currently visible depots. You can narrow your search by using the optional arguments to filter the output.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

3 Create a new profile, assign it a name and vendor, and add a base package.

```
New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-
base[0],esx-xlibs[0]
```

The example uses the esx-base package. In most cases, you include the esx-base package when you create a new image profile. Names that contain spaces are surrounded by quotes.

4 Use a pipeline to pass 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 at thevSphere PowerCLI prompt.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage
$pkgs[0]
$ip2.VibList | format-list
```

Edit 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 might prevent the image profile from working correctly, an error occurs.

Prerequisites

- vSphere PowerCLI and prerequisite software is installed. See "Install vSphere ESXi Image Builder and Prerequisite Software," on page 145.
- 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.

Procedure

1 In a vSphere PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
ZIP file	a Download the ZIP file to a local file system. b Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2 Use a pipeline to pass the image profile you intend to edit to `format-list` to see detailed information.

In this example, the image profile created in "Create New Image Profiles Workflow," on page 157 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 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 that of the image profile, 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
```

Note If an error occurs when you add the software package, you might have a problem with acceptance levels, see "Working with Acceptance Levels," on page 152

5 View 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 by Using 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 vSphere 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 5

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

This chapter includes the following topics:

ESXi Autoconfiguration

When you turn on the ESXi host for the first time or after resetting the configuration defaults, the host enters an autoconfiguration phase. This phase configures system network and storage devices with default settings.

By default, Dynamic Host Configuration Protocol (DHCP) configures IP, and all visible blank internal disks are formatted with the virtual machine file system (VMFS) so that virtual machines can be stored on the disks.

About the Direct Console ESXi Interface

Use the direct console interface for initial ESXi configuration and troubleshooting.

Connect a keyboard and monitor to the host to use the direct console. After the host completes the autoconfiguration phase, the direct console appears on the monitor. You can examine the default network configuration and change any settings that are not compatible with your network environment.

Key operations available to you in the direct console include:

- Configuring hosts
- Setting up administrative access
- Troubleshooting

You can also use vSphere Web Client to manage the host by using vCenter Server.

Table 5-1. 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
View the VMkernel log	Alt+F12
Switch to the shell console	Alt+F1
Switch to the direct console user interface	Alt+F2
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 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Click the **Manage** tab.

4 Click **Settings**.

5 Under System, select **Advanced System Settings**.

6 Select **Annotations**.

7 Click the Edit icon.

8 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 163

  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 from the vSphere Web Client on page 164

  You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Web Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

- Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy on page 164

  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 from the vSphere Web Client," on page 164

Redirect the Direct Console to a Serial Port from the vSphere Web Client

You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Web Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

Prerequisites

- Verify that you can access the host from the vSphere Web Client.
- Verify that the serial port is not in use for serial logging and debugging, or for ESX Shell (tty1Port).

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Click the **Manage** tab.

4 Click **Settings**.

5 Under System, select **Advanced System Settings**.

6 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.

7 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: **`com1`** or **`com2`.**

8 Reboot the host.

You can now manage the ESXi host remotely from a console that is connected to the serial port.

Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy

After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

Prerequisites

The serial port must not already be in use for serial logging and debugging.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Click the **Manage** tab.

4 Select **Settings**.

5 Select **Advanced System Settings**.

6 Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.

7 Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: `com1` or `com2.`

8 Click **OK**.

9 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.

Change the BIOS Boot Setting for ESXi

Configure the BIOS boot setting for ESXi if you want the server to boot into ESXi by default.

ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1 While the ESXi host is powering on, press the key required to enter your host's BIOS setup.

Depending on your server hardware, the key might be a function key or Delete. The option to enter the BIOS setup might be different for your server.

2 Select the BIOS boot setting.

Option	Description
If you are using the installable version of ESXi	Select the disk on which you installed the ESXi software and move it to the first position in the list. The host boots into ESXi.
If you are using ESXi Embedded	Select the USB flash device and move it to the first position in the list. The host starts in ESXi mode.

Configure the Boot Setting for Virtual Media

If you are using remote management software to set up ESXi, you might need to configure the boot setting for virtual media.

Virtual media is a method of connecting a remote storage media such as CD-ROM, USB mass storage, ISO image, and floppy disk to a target server that can be anywhere on the network. The target server has access to the remote media, and can read from and write to it as if it were physically connected to the server's USB port.

Prerequisites

ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1 Connect the media to the virtual device.

For example, if you are using a Dell server, log in to the Dell Remote Access Controller (DRAC) or a similar remote management interface and select a physical floppy or CD-ROM drive, or provide a path to a floppy image or CD-ROM image.

2 Reboot the server.

3 While the server is powering on, enter the device selection menu.

Depending on your server hardware, the key might be a function key or Delete.

4 Follow the instructions to select the virtual device.

The server boots from the configured device once and goes back to the default boot order for subsequent boots.

Host Fails to Boot After You Install ESXi in UEFI Mode

When you install ESXi on a host machine in UEFI mode, the machine might fail to boot.

Problem

When you reboot after installing ESXi on a host machine in UEFI mode, the reboot might fail. This problem is accompanied by an error message similar to `Unexpected network error. No boot device available.`

Cause

The host system fails to recognize the disk that ESXi is installed on as the boot disk.

Solution

1 While the error message is displayed on screen, press F11 to display boot options.

2 Select an option similar to **Add boot option**.

The wording of the option might vary, depending on your system.

3 Select the file `\EFI\BOOT\BOOTx64.EFI` on the disk that you installed ESXi on.

4 Change the boot order so that the host boots from the option that you added.

Network Access to Your ESXi Host

The default behavior is to configure the ESXi management network using DHCP. You can override the default behavior and use static IP settings for the management network after the installation is completed.

Table 5-2. 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 Web Client and customize settings, including changing the management IP address.
One of the following is true: ■ You do not have a DHCP server. ■ The ESXi host is not connected to a DHCP server. ■ Your connected DHCP server is not functioning properly.	During the autoconfiguration phase, the software assigns the link local IP address, which is in the subnet 169.254.x.x/16. The assigned IP address appears on the direct console. You can override the link local IP address by configuring a static IP address using the direct console.
The ESXi host is connected to a functioning DHCP server, but you do not want to use the DHCP-configured IP address.	During the autoconfiguration phase, the software assigns a DHCP-configured IP address. You can make the initial connection by using the DHCP-configured IP address. Then you can configure a static IP address. If you have physical access to the ESXi host, you can override the DHCP-configured IP address by configuring a static IP address using the direct console.
Your security deployment policies do not permit unconfigured hosts to be powered on the network.	Follow the setup procedure in “Configure the Network Settings on a Host That Is Not Attached to the Network,” on page 167.

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 user interface to configure the password for the administrator account (root).

3 Use the direct console user interface to configure a static IP address.

4 Connect a network cable to the host.

5 (Optional) Use the vSphere Web 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 your ESXi hosts.

For instructions about downloading and installing vCenter Server and the vCenter Server components or for downloading and deploying the vCenter Server Appliance, see Chapter 8, "Installing vCenter Server on a Windows Virtual Machine or Physical Server," on page 223 and Chapter 9, "Deploying the vCenter Server Appliance," on page 233. For instructions about installing the vSphere Client, see "Install the vSphere Client," on page 183.

Configuring Network Settings

ESXi requires one IP address for the management network. To configure basic network settings, use the vSphere Web Client or the direct console.

Use the vSphere Web Client if you are satisfied with the IP address assigned by the DHCP server.

Use the direct console for network configuration 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.

ESXi Networking Security Recommendations

Isolation of network traffic is essential to a secure ESXi environment. Different networks require different access and level of isolation.

Your ESXi host uses several networks. Use appropriate security measures for each network, and isolate traffic for specific applications and functions. For example, ensure that vSphere vMotion traffic does not travel over networks where virtual machines are located. Isolation prevents snooping. Having separate networks also is recommended for performance reasons.

- vSphere infrastructure networks are used for features such as VMware vSphere vMotion®, VMware vSphere Fault Tolerance, and storage. These networks are considered to be isolated for their specific functions and often are not routed outside a single physical set of server racks.
- A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from normal traffic. This network should be accessible only by system, network, and security administrators. Use jump box or virtual private network (VPN) to secure access to the management network. Strictly control access within this network to potential sources of malware.
- Virtual machine traffic can flow over one or many networks. You can enhance the isolation of virtual machines by using virtual firewall solutions that set firewall rules at the virtual network controller. These settings travel with a virtual machine as it migrates from host to host within your vSphere environment.

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 vCenter Server and SNMP client. Network adapters on the host are named vmnic*N*, where N is a unique number identifying the network adapter, for example, vmnic0, vmnic1, and so forth.

During the autoconfiguration phase, the ESXi host chooses vmnic0 for management traffic. You can override the default choice by manually choosing the network adapter that carries management traffic for the host. In some cases, you might want to use a Gigabit Ethernet network adapter for your management traffic. Another way to help ensure availability is to select multiple network adapters. Using multiple network adapters enables load balancing and failover capabilities.

Procedure

1 From the direct console, select **Configure Management Network** and press Enter.

2 Select **Network Adapters** and press Enter.

3 Select a network adapter and press Enter.

After the network is functional, you can use the vSphere Web Client to connect to the ESXi host through vCenter Server.

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 53

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 Web Client

If you do not have physical access to the host, you can use the vSphere Web Client to configure static IP settings.

Procedure

1 Log in to the vCenter Server from the vSphere Web Client.

2 Select the host in the inventory.

3 On the **Manage** tab, select **Networking**.

4 Select **Virtual adapters**.

5 Select **vmk0 Management Network** and click the edit icon.

6 Select **IPv4 settings**.

7 Select **Use static IPv4 settings**.

8 Enter or change the static IPv4 address settings.

9 (Optional) Set static IPv6 addresses.

   a Select **IPv6 settings**.

   b Select **Static IPv6 addresses**.

   c Click the add icon.

   d Type the IPv6 address and click **OK**.

10 Click **OK**.

Configuring DNS for ESXi

You can select either manual or automatic DNS configuration of the ESXi host.

The default is automatic. For automatic DNS to work, your network environment must have a DHCP server and a DNS server.

In network environments where automatic DNS is not available or not desirable, you can configure static DNS information, including a host name, a primary name server, a secondary name server, and DNS suffixes.

Configure DNS Settings from the Direct Console

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

Procedure

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

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

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

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

Configure DNS Suffixes

If you have physical access to the host, you can use the direct console to configure DNS information. By default, DHCP acquires the DNS suffixes.

Procedure

1 From the direct console, select **Configure Management Network**.

2 Select **Custom DNS Suffixes** and press Enter.

3 Enter new DNS suffixes.

Test the Management Network

You can use the direct console to do simple network connectivity tests.

The direct console performs the following tests.

- Pings the default gateway
- Pings the primary DNS name server
- Pings the secondary DNS nameserver
- Resolves the configured host name

Procedure

1 From the direct console, select **Test Management Network** and press Enter.

2 Press Enter to start the test.

Restart the Management Agents

The management agents synchronize VMware components and let you access the ESXi host by using the vSphere Web Client and vCenter Server. They are installed with the vSphere software. You might need to restart the management agents if remote access is interrupted.

Restarting the management agents restarts all management agents and services that are installed and running in `/etc/init.d` on the ESXi host. Typically, these agents include hostd, ntpd, sfcbd, slpd, wsman, and vobd. The software also restarts the Fault Domain Manager (FDM) if installed.

Users accessing this host by using the vSphere Web Client and 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.

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.

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 5-3.

Table 5-3. Partitions Created by ESXi on the Host Drive

ESXi Version	Partitions Created
ESXi Installable	For fresh installations, several new partitions are created for the boot banks, the scratch partition, and the locker. Fresh ESXi installations use GUID Partition Tables (GPT) instead of MSDOS-based partitioning. The partition table itself is fixed as part of the binary image, and is written to the disk at the time the system is installed. The ESXi installer leaves the scratch and VMFS partitions blank and ESXi creates them when the host is rebooted for the first time after installation or upgrade. One 4GB VFAT scratch partition is created for system swap. See "About the Scratch Partition," on page 174. The VFAT scratch partition is created only on the disk from which the ESXi host is booting. **Note** To create the VMFS volume and a scratch partition with the installation, the ESXi installer requires a minimum of 5.2GB of free space on the installation disk. The installer affects only the installation disk. The installer does not affect other disks of the server. When you install on a disk, the installer overwrites the entire disk. When the installer autoconfigures storage, the installer does not overwrite hardware vendor partitions. During ESXi installation, the installer creates a 110MB diagnostic partition for core dumps.
ESXi Embedded	One 110MB diagnostic partition for core dumps, if this partition is not present on another disk. The VFAT scratch and diagnostic partitions are created only on the disk from which the ESXi host is booting. On other disks, the software creates one VMFS5 partition per blank disk, using the whole disk. Only blank disks are formatted.
Both ESXi Installable and ESXi Embedded	One VMFS5 partition on the remaining free space.

You might want to override this default behavior if, for example, you use shared storage devices instead of local storage. To prevent automatic disk formatting, detach the local storage devices from the host under the following circumstances:

- Before you start the host for the first time.

- Before you start the host after you reset the host to the configuration defaults.

To override the VMFS formatting if automatic disk formatting already occurred, you can remove the datastore. See the *vCenter Server and Host Management* documentation.

About the Scratch Partition

For new installations of ESXi, during the autoconfiguration phase, a 4GB VFAT scratch partition is created if the partition is not present on another disk.

Note Partitioning for hosts that are upgraded to ESXi 5.x from ESXi versions earlier than version 5.0 differs significantly from partitioning for new installations of ESXi 5.x. See the *vSphere Upgrade* documentation.

When ESXi boots, the system tries to find a suitable partition on a local disk to create a scratch partition.

The scratch partition is not required. It is used to store vm-support output, which you need when you create a support bundle. If the scratch partition is not present, vm-support output is stored in a ramdisk. In low-memory situations, you might want to create a scratch partition if one is not present.

For the installable version of ESXi, the partition is created during installation and is selected. VMware recommends that you do not modify the partition.

Note To create the VMFS volume and scratch partition, the ESXi installer requires a minimum of 5.2GB of free space on the installation disk.

For ESXi Embedded, if a partition is not found, but an empty local disk exists, the system formats it and creates a scratch partition. If no scratch partition is created, you can configure one, but a scratch partition is not required. You can also override the default configuration. You might want to create the scratch partition on a remote NFS mounted directory.

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

Set the Scratch Partition from the vSphere Web 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. From the vSphere Web Client, connect to the vCenter Server.
2. Select the host in the inventory.
3. Click the **Manage** tab.
4. Select **Settings**.
5. Select **Advanced System Settings**.

   The setting **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. From the vSphere Web Client, connect to the vCenter Server.
3. Select the host in the inventory.
4. Click the **Manage** tab.
5. Click **Settings**.
6. Under System, select **Advanced System Settings**.
7. Select **ScratchConfig**.

   The field **ScratchConfig.CurrentScratchLocation** shows the current location of the scratch partition.
8. In the field **ScratchConfig.ConfiguredScratchLocation**, enter a directory path that is unique for this host.
9. 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 176.

Configure Syslog on ESXi Hosts

All ESXi hosts run a syslog service (`vmsyslogd`), which logs messages from the VMkernel and other system components to log files.

You can use the vSphere Web 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 Web Client inventory, select the host.

2 Click the **Manage** tab.

3 In the System panel, click **Advanced System Settings**.

4 Locate the **Syslog** section of the Advanced System Settings list.

5 To set up logging globally, select the setting to change and click the Edit icon.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified as [*datastorename*] *path_to_file* where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:1514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

6 (Optional) To overwrite the default log size and log rotation for any of the logs.

   a Click the name of the log you that want to customize.

   b Click the Edit icon and enter the number of rotations and log size you want.

7 Click **OK**.

Changes to the syslog options take effect immediately.

Enable ESXi Shell and SSH Access with the Direct Console User Interface

Use the direct console user interface to enable the ESXi Shell.

Procedure

1 From the Direct Console User Interface, press F2 to access the System Customization menu.

2 Select **Troubleshooting Options** and press Enter.

3 From the Troubleshooting Mode Options menu, select a service to enable.

- Enable ESXi Shell
- Enable SSH

4 Press Enter to enable the service.

5 (Optional) Set the timeout for the ESXi Shell.

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

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

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

a From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.

b Enter the availability timeout in minutes.

The availability timeout is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled.

c Press Enter.

d Enter the idle timeout.

The idle timeout is the number of minutes that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the ESXi Shell and do not affect existing sessions.

6 Press Esc until you return to the main menu of the Direct Console User Interface.

Set the Host Image Profile Acceptance Level

The Host Image Profile acceptance level determines which vSphere installation bundles (VIBs) are accepted for installation.

VIB signatures are checked and accepted for installation based on a combination of the VIB acceptance level and the host image profile acceptance level. VIBs are tagged with an acceptance level that depends on their signature status.

See "Acceptance Levels," on page 141.

Prerequisites

Required privileges: **Host.Configuration.SecurityProfile** and **Host.Configuration.Firewall**

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Click the **Manage** tab.

4 Click **Settings**.

5 Under System, select **Security Profile**.

6 Scroll down to Host Image Profile Acceptance Level, and click **Edit**.

7 Select the acceptance level and click **OK**.

Table 5-4. Host Image Profile Acceptance Levels

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMware Certified	VMware Certified
VMware Accepted	VMware Certified, VMware Accepted
Partner Supported	VMware Certified, VMware Accepted, Partner Supported
Community Supported	VMware Certified, VMware Accepted, Partner Supported, Community Supported

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.

Decommission an ESXi Host

If you do not want your server to be an ESXi host, you can decommission the ESXi host machine.

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 6

After ESXi is installed and set up, you can manage the host by using the vSphere Web Client and vCenter Server, license the host, and back up your ESXi configuration.

You can also use the vSphere Client to connect directly to the ESXi host and to manage it.

This chapter includes the following topics:

- "Managing the ESXi Host," on page 181
- "Licensing ESXi Hosts," on page 181
- "Install the vSphere Client," on page 183

Managing the ESXi Host

The vSphere Client provides the simplest way to manage your ESXi host and operate its virtual machines.

You can also use the vSphere Web Client to connect to and manage vCenter Server by using a Web browser. The vSphere Web Client is installed together with vCenter Server and the vCenter Server Appliance and you can use it to manage your ESXi hosts.

Licensing ESXi Hosts

After you install ESXi, it has a 60-day evaluation period during which you can explore the full set of vSphere features provided with a vSphere Enterprise Plus license. You must assign the host an appropriate license before the evaluation period expires.

ESXi hosts are licensed with vSphere licenses that have per-CPU capacity. To license hosts correctly, you must assign them a vSphere license that has enough CPU capacity to cover all CPUs in the hosts. The license must support all features that the hosts are using. For example, if the hosts are connected to a vSphere Distributed Switch, you must assign a license that has the vSphere Distributed Switch feature.

You can use one of following methods to license ESXi hosts:

- License multiple hosts at a time by using the license management function in the vSphere Web Client. The hosts must be connected to a vCenter Server system. For more information, see *vCenter Server and Host Management*.
- Set up bulk licensing by 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 85
- License individual ESXi hosts through a direct connection with the vSphere Client. For more information, see *vSphere Administration with the vSphere Client*.

About ESXi Evaluation and Licensed Modes

You can use evaluation mode to explore the entire set of features for ESXi hosts. The evaluation mode provides the set of features equal to a vSphere Enterprise Plus license. Before the evaluation mode expires, you must assign to your hosts a license that supports all the features in use.

For example, in evaluation mode, you can use vSphere vMotion technology, the vSphere HA feature, the vSphere DRS feature, and other features. If you want to continue using these features, you must assign a license that supports them.

The installable version of ESXi hosts is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal storage 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. At any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. The time available in the evaluation period is decreased by the time already used.

For example, suppose that you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard Edition license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features for the host for the remaining evaluation period of 40 days.

For information about managing licensing for ESXi hosts, see the *vCenter Server and Host Management* documentation.

Recording the License Key of an ESXi Host

If a host becomes inaccessible or unbootable, you should have a record of its license key. You can write down the license key and tape it to the server, or put the license key in a secure location. You can access the license key from the direct console user interface or the vSphere Web Client.

View the License Keys of ESXi Hosts from the vSphere Web Client

You can view the license keys of the hosts that are connected to a vCenter Server system through the vSphere Web Client.

Procedure

1. In the vSphere Web Client, select **Administration**.
2. Under Licensing, select **Licenses**.
3. On the **Assets** tab, select **Hosts**.
4. In the License column, click a license.

You view information about the license, such as its usage and 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.

Install the vSphere Client

The vSphere Client enables you to connect to an ESXi host.

Prerequisites

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

Procedure

1 Run the vSphere Client installer in one of the following ways.

Option	Description
If you are installing from the vCenter Server installer	a In the software installer directory, double-click the `autorun.exe` file. b Select **vSphere™ Client**. c Click **Install**.
If you downloaded the vSphere Client	Double-click the `VMware-viclient-`*`build number`*`.exe` file.

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

You can use the vSphere Client to connect to an ESXi host or to connect to a vCenter Server system.

Before You Install vCenter Server or Deploy the vCenter Server Appliance 7

You can install vCenter Server on a physical system or on a virtual machine running on an ESXi host. You can also download and deploy the vCenter Server Appliance on a host running ESXi 5.0 or later.

This chapter includes the following topics:

Preparing vCenter Server Databases

vCenter Server requires a database to store and organize server data. You can either use the bundled PostgreSQL database that can be installed and configured at deployment time, or you can set up an external database.

vCenter Server for Windows supports Oracle and Microsoft SQL database, while the vCenter Server Appliance supports only an Oracle database as an external database.

Although the database is automatically configured by the installer, you can configure an external database manually or by using a script. In addition, the data source name user must have a specific list of permissions.

See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 189 and "Configure an Oracle Database User," on page 198.

The database passwords are stored in clear text on the Windows virtual machine or physical host on which you install vCenter Server and in the vCenter Server Appliance. The files containing the passwords are protected by using the operating system protection, that is, you must be a Windows local administrator or a Linux root user to access and read these files.

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 cannot install vCenter Server and point to an older external vCenter Server database. You can upgrade the vCenter Server 5.x database to the latest version only by upgrading the vCenter Server instance connected to that database. For information about upgrading vCenter Server, see *vSphere Upgrade*.

vCenter Server Database Configuration Notes

After you select a supported database type, make sure you understand any special configuration requirements.

Table 7-1 is not a complete list of databases supported with vCenter Server and the vCenter Server Appliance. For information about specific database versions and service pack configurations supported with vCenter Server, see the VMware Product Interoperability Matrixes. The vCenter Server Appliance supports the same Oracle database versions as vCenter Server. Only special database configuration notes not listed in the Product Interoperability Matrixes are provided in Table 7-1.

vCenter Server databases require a UTF code set.

Contact your DBA for the appropriate database credentials.

Table 7-1. Configuration Notes for Databases Supported with vCenter Server

Database Type	Configuration Notes
PostgreSQL	For vCenter Server 6.0, the bundled PostgreSQL database is suitable for environments with up to 20 hosts and 200 virtual machines. For the vCenter Server Appliance, you can use the embedded PostgreSQL database for environments with up to 1,000 hosts and 10,000 virtual machines. IMPORTANT If you use the embedded PostgreSQL database, uninstalling vCenter Server on Windows, uninstalls the embedded database, and all data is lost.
Microsoft SQL Server 2008 R2 SP2 or higher	Ensure that the machine has a valid ODBC DSN entry. NOTE This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2012	Ensure that the machine has a valid ODBC DSN entry. NOTE This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2014	Ensure that the machine has a valid ODBC DSN entry. NOTE This database is not supported for the vCenter Server Appliance.
Oracle 11g and Oracle 12c	Ensure that the machine has a valid ODBC DSN entry. After you complete the vCenter Server installation, apply the latest patch to the Oracle client and server.

Create a 64-Bit DSN

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

NOTE Your SQL database might have certain requirements for the ODBC driver. See Knowledge Base article 1015804.

Procedure

1 From the Windows Start menu, select **Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Create a system DSN.

If you have a Microsoft SQL database, create the system DSN by using SQL Native Client version 10 or 11.

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.

Verify That vCenter Server Can Communicate with the Local Database

If your database is located on the same machine on which vCenter Server is to be installed, and you have changed the name of this machine, verify the configuration. Make sure that 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.

If your database is remote, you can skip this procedure. The name change has no effect on communication with remote databases.

After you rename the server, verify with your database administrator or the database vendor that all components of the database are working.

Prerequisites

- Make sure that the database server is running.
- Make sure that the vCenter Server computer name is updated in the domain name service (DNS).

Procedure

1. Update the data source information, as needed.
2. Ping the computer name to test this connection.

   For example, if the computer name is `host-1.company.com`, run the following command at the Windows command prompt:

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

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

vCenter Server communication is confirmed. You can continue to prepare other components of your environment.

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 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 188

   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 189

By using this method, available with vCenter Server 5.x and later, 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 190

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 Server 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 191

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 and Apply a Microsoft SQL Server Database Schema and Roles on page 191

In this method of configuring the SQL database, you create the custom schema VMW, instead of using the existing dbo schema. You must also enable Database Monitoring for a user before you install vCenter Server with an embedded or external Platform Services Controller.

6 (Optional) Use a Script to Create Microsoft SQL Server Database Objects Manually on page 193

You can create database objects manually with this method of configuring the SQL database.

7 Configure a SQL Server ODBC Connection on page 195

After you create a vCenter Server user, establish a connection with a SQL Server database. This connection is required to install a vCenter Server instance.

8 Configure Microsoft SQL Server TCP/IP for JDBC on page 197

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.

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>/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
use [master]
go
CREATE DATABASE [VCDB] ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\db\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\db\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
```

```
go
CREATE LOGIN [vpxuser] WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use MSDB
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
```

You now have a Microsoft SQL Server database that you can use with vCenter Server.

What to do next

See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 189.

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

By using this method, available with vCenter Server 5.x and later, the vCenter Server database administrator can set permissions for vCenter Server users and administrators to be granted through Microsoft SQL Server database roles.

Use this method because it removes the requirement to set up the database dbo schema and db_owner role for vCenter Server users who install and upgrade vCenter Server.

Alternatively, you can assign vCenter Server database permissions by creating and assigning the db_owner role and letting the vCenter Server installer create the default schema that assigns database user permissions to that role. See "Set Database Permissions by Using the dbo Schema and the db_owner Database Role," on page 190.

Prerequisites

Create the vCenter Server database. See "Create a SQL Server Database and User for vCenter Server," on page 188

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 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 role.
6. In the vCenter Server database, grant the schema permissions SELECT, INSERT, DELETE, UPDATE, and EXECUTE to the VC_USER_ROLE role.
7. Grant the VC_USER_ROLE role to the user [vpxuser].
8. Grant the VC_ADMIN_ROLE role to the user [vpxuser].
9. In the MSDB database, create the user [vpxuser].
10. In the MSDB database, create the VC_ADMIN_ROLE role.

11 Grant privileges to the VC_ADMIN_ROLE role in MSDB .

    a On the MSDB tables syscategories, sysjobsteps, sysjobs_view, 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, sp_add_category, and sp_lock grant the EXECUTE permission to the VC_ADMIN_ROLE role.

12 In the MSDB database, grant the VC_ADMIN_ROLE role to the user [vpxuser].

13 Grant the permissions VIEW SERVER STATE and VIEW ANY DEFINITIONS to the user [vpxuser].

14 Connect to the vCenter Server database as user [vpxuser] and create the ODBC DSN.

15 Install vCenter Server.

16 In the MSDB database, revoke the VC_ADMIN_ROLE role from the user [vpxuser].

    After you revoke the role, you can leave the role as inactive for use in future upgrades, or remove the role for increased security. If you remove the role, you must create the role again and assign it to the user [vpxuser] before any future upgrade of vCenter Server.

The hardcoded dbo role is removed from `VCDB_mssql.sql`.

What to do next

"Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles," on page 191

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 Server 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 189 and "Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles," on page 191. 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 188

Procedure

1 Assign the dbo role 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 189"Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles," on page 191. 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 dbo database role 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 188

Procedure

1 Log in to a Microsoft SQL Server Management Studio session as the sysadmin or a user account with **sysadmin** privileges.

2 Run the script to create a vCenter Server user.

  The script is located in the vCenter Server installation package `/`*`installation directory`*`/vCenter-Server/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 195

Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles

In this method of configuring the SQL database, you create the custom schema VMW, instead of using the existing dbo schema. You must also enable Database Monitoring for a user before you install vCenter Server with an embedded or external Platform Services Controller.

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 189 and "Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles," on page 191.

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 188

Procedure

1 Log in to a Microsoft SQL Server Management Studio session as the sysadmin or a user account with sysadmin privileges.

2 Run the following script to create the database schema and roles.

The script is located in the vCenter Server installation package at `/*installation directory*/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt` .

```
CREATE SCHEMA [VMW]
go
ALTER USER [vpxuser] WITH DEFAULT_SCHEMA =[VMW]

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 SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLEg
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
GRANT EXECUTE ON msdb.dbo.sp_lock TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use master
go
grant VIEW SERVER STATE to [vpxuser]
go
GRANT VIEW ANY DEFINITION TO [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 195.

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 190 and "Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role," on page 191.
- Grant the VC_ADMIN_ROLE role to the database *user* in VCDB and in MSDB, and grant the VC_USER_ROLE role to the database *user* in VCDB. See "Set Database Permissions By Manually Creating Database Roles and the VMW Schema," on page 189.

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 188

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 `VCDB_mssql.SQL` and the `Topn_DB_mssql.sql` files by using Microsoft SQL Server Management Studio and replace all occurrences of `$schema` with the schema name.

4 Open `VCDB_views_mssql.sql` file by using Microsoft SQL Server Management Studio and replace all occurrences of `;` with `;` new line, and `go`.

5 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
insert_stats_proc_mssql.sql
load_stats_proc_mssql.sql
purge_stat2_proc_mssql.sql
purge_stat3_proc_mssql.sql
purge_usage_stats_proc_mssql.sql
stats_rollup1_proc_mssql.sql
stats_rollup2_proc_mssql.sql
stats_rollup3_proc_mssql.sql
cleanup_events_mssql.sql
delete_stats_proc_mssql.sql
upsert_last_event_proc_mssql.sql
load_usage_stats_proc_mssql.sql
TopN_DB_mssql.sql
calc_topn1_proc_mssql.sql
calc_topn2_proc_mssql.sql
calc_topn3_proc_mssql.sql
calc_topn4_proc_mssql.sql
clear_topn1_proc_mssql.sql
clear_topn2_proc_mssql.sql
clear_topn3_proc_mssql.sql
clear_topn4_proc_mssql.sql
rule_topn1_proc_mssql.sql
rule_topn2_proc_mssql.sql
rule_topn3_proc_mssql.sql
rule_topn4_proc_mssql.sql
process_license_snapshot_mssql.sql
l_stats_rollup3_proc_mssql.sql
l_purge_stat2_proc_mssql.sql
l_purge_stat3_proc_mssql.sql
l_stats_rollup1_proc_mssql.sql
l_stats_rollup2_proc_mssql.sql
VCDB_views_mssql.sql
```

6 (Optional) You can also run the following scripts to enable database health monitoring.

```
job_dbm_performance_data_mssql.sql
process_performance_data_mssql.sql
```

7 For all supported editions of Microsoft SQL Server (except Microsoft SQL Server 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
```

8 For all the procedures you created in Step 5, grant the execute privilege to the vCenter Server database.

```
grant execute on insert_stats_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_proc to vCenter_db_user
grant execute on l_stats_rollup3_proc to vCenter_db_user
grant execute on l_purge_stat2_proc to vCenter_db_user
grant execute on l_purge_stat3_proc to vCenter_db_user
grant execute on l_stats_rollup1_proc to vCenter_db_user
grant execute on l_stats_rollup2_proc to vCenter_db_user
```

If you ran the script `process_performance_data_mssql.sql` in Step 5, grant the following execute privilege to the vCenter Server database.

```
grant execute on process_performance_data_proc to vCenter_db_user
```

9 On the machine on which you intend to install vCenter Server, create a DSN that points to the database server with the schema.

10 Run the vCenter Server installer.

11 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.

12 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 instance.

If you use SQL Server for vCenter Server, do not use the master database.

See your Microsoft SQL ODBC documentation for specific instructions for configuring the SQL Server ODBC connection.

⚠ CAUTION If you are using a named instance of Microsoft SQL Server 2008 Standard Edition with vCenter Server, do not name the instance MSSQLSERVER. If you do, the JDBC connection does not work, and certain features, such as Performance Charts, are not available.

Prerequisites

- Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 186.
- 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 188.
- 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 189 and "Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles," on page 191.
  - Option 2 (alternative): Follow the procedures in "Set Database Permissions by Using the dbo Schema and the db_owner Database Role," on page 190 and "Use a Script to Create a vCenter Server User by Using the dbo Schema and db_owner Database Role," on page 191.
- Deploy SQL Native Client version 10 or 11.

Procedure

1. On your vCenter Server system, select **Start > Administrative Tools > Data Sources (ODBC)**.
2. On the **System DSN** tab, modify an existing or create a new SQL Server ODBC connection.
   - To modify an existing SQL Server ODBC connection, select the connection from the System Data Source list and click **Configure**.

     IMPORTANT The existing DSN must use SQL Native Client version 10 or 11.

   - To create a new SQL Server ODBC connection, click **Add**, select **SQL Native Client**, and click **Finish** .
3. Type an ODBC data source 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 an authentication method.
   - **Integrate Windows authentication**.

     Additionally, you can also enter the Service Principal Name (SPN).

     IMPORTANT You cannot use this option if the vCenter Server service is running under the Microsoft Windows built-in system account.

   - **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 2008 editions, test the data source by selecting **Test Data Source** and clicking **OK** from the **ODBC Microsoft SQL Server Setup** menu.

10 Verify that the SQL Agent is running on your database server.

Configure Microsoft SQL Server TCP/IP for JDBC

If the Microsoft SQL Server database has TCP/IP disabled and the dynamic ports are not set, the JDBC connection remains closed. The closed connection causes the vCenter Server statistics to malfunction. You can configure the server TCP/IP for JDBC.

This task applies to remote Microsoft SQL Server database servers. You can skip this task if your database is local.

Procedure

1 Select **Start > All Programs > Microsoft SQL Server > Configuration Tool > SQL Server Configuration Manager**.

2 Select **SQL Server Network Configuration > Protocols for *Instance name***.

3 Enable TCP/IP.

4 Open TCP/IP Properties.

5 On the **Protocol** tab, make the following entries.

Enabled	**Yes**
Listen All	**Yes**
Keep Alive	**30000**

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

Active	**Yes**
TCP Dynamic Ports	**0**

7 Restart the SQL Server service from **SQL Server Configuration Manager > SQL Server Services**.

8 Start the SQL Server Browser service from **SQL Server Configuration Manager > SQL Server Services**.

What to do next

Optionally, you can enable Database Monitoring for Microsoft SQL database users. Otherwise, install vCenter Server.

Configure Oracle Databases

To use an Oracle database for your vCenter Server repository, configure your database to work with vCenter Server.

Procedure

1 Use a Script to Create a Local or Remote Oracle Database on page 198

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.

2 Configure an Oracle Database User on page 198

To use an Oracle database when you install vCenter Server, you must configure the database user.

3 (Optional) Configure an Oracle Database User to Enable Database Monitoring on page 200

   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.

4 (Optional) Use a Script to Create the Oracle Database Schema on page 200

   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.

5 Configure an Oracle Connection for Local Access on page 202

   Configure a connection for local access if you install vCenter Server on the same system as the Oracle database.

6 Configure an Oracle Database Connection for Remote Access on page 202

   Before a vCenter Server system can access the Oracle database remotely, you must configure an Oracle connection.

7 Connect to an Oracle Database Locally on page 203

   Before a vCenter Server system can connect to an Oracle database locally, you must set up the connection.

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`*`/vCenter-Server/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.

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/vCenter-Server/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_lock 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 select on v_$session 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.

(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.

(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 202 or "Configure an Oracle Database Connection for Remote Access," on page 202, 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/vCenter-Server/dbschema` directory.

3 In SQL*Plus, run the scripts in sequence on the database.

path is the directory path to the `/installation directory/vCenter-Server/dbschema` folder.

```
@path/VCDB_oracle.SQL
@path/VCDB_views_oracle.SQL
@path/insert_stats_proc_oracle.sql
@path/load_stats_proc_oracle.sql
@path/purge_stat2_proc_oracle.sql
@path/purge_stat3_proc_oracle.sql
@path/purge_usage_stats_proc_oracle.sql
@path/stats_rollup1_proc_oracle.sql
@path/stats_rollup2_proc_oracle.sql
```

```
@path/stats_rollup3_proc_oracle.sql
@path/cleanup_events_oracle.sql
@path/delete_stats_proc_oracle.sql
@path/load_usage_stats_proc_oracle.sql
@path/TopN_DB_oracle.sql
@path/calc_topn1_proc_oracle.sql
@path/calc_topn2_proc_oracle.sql
@path/calc_topn3_proc_oracle.sql
@path/calc_topn4_proc_oracle.sql
@path/clear_topn1_proc_oracle.sql
@path/clear_topn2_proc_oracle.sql
@path/clear_topn3_proc_oracle.sql
@path/clear_topn4_proc_oracle.sql
@path/rule_topn1_proc_oracle.sql
@path/rule_topn2_proc_oracle.sql
@path/rule_topn3_proc_oracle.sql
@path/rule_topn4_proc_oracle.sql
@path/process_license_snapshot_oracle.sql
@path/l_purge_stat2_proc_oracle.sql
@path/l_purge_stat3_proc_oracle.sql
@path/l_stats_rollup1_proc_oracle.sql
@path/l_stats_rollup2_proc_oracle.sql
@path/l_stats_rollup3_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
```

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.

9 When prompted, provide the database user login.

The Oracle database schema is created.

Configure an Oracle Connection for Local Access

Configure a connection for local access if you install vCenter Server on the same system as the Oracle database.

Prerequisites

Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 186. If you do not prepare your database correctly, the vCenter Server installer displays error and warning messages.

Procedure

1 Download Oracle 11g or Oracle 12c from the Oracle Web site.

2 Install Oracle 11g or Oracle 12c, and create a database.

3 Configure the TNS Service Name option in the ODBC DSN.

   The TNS Service Name is the net service name for the database to which you want to connect. You can find the net service name in the `tnsnames.ora` file located in the `NETWORK\ADMIN` folder in the Oracle database installation location.

The database is configured for local access.

Configure an Oracle Database Connection for Remote Access

Before a vCenter Server system can access the Oracle database remotely, you must configure an Oracle connection.

Prerequisites

Review the required database patches specified in "vCenter Server Database Configuration Notes," on page 186. If you do not prepare your database correctly, the vCenter Server installer displays error and warning messages.

Procedure

1 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)
   )
   )
```

2 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

- 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

You can enable Database Monitoring for Oracle database users. Otherwise, install vCenter Server.

Database Permission Requirements for vCenter Server

vCenter Server requires a database. If you decide to use an external Oracle or Microsoft SQL Server database, when you create the database, you must grant certain permissions to the database user.

Table 7-2. Microsoft SQL Database Permissions for vCenter Server

Permission	Description
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Mandatory when you work with SQL Server custom schema.
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Mandatory when you work with SQL Server custom schema.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Mandatory when you work with SQL Server custom schema.
GRANT CREATE TABLE TO VC_ADMIN_ROLE	Necessary for creating a table.
GRANT CREATE VIEW TO VC_ADMIN_ROLE	Necessary for creating a view.
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	Necessary for creating a stored procedure.
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	Permissions that let you run SELECT, INSERT, DELETE, UPDATE operations on tables which are part of the VMW schema.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Necessary for running a stored procedure in the db schema.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Necessary for deploying SQL Server jobs. These permissions are mandatory only during installation and upgrade and not required after deployment.
GRANT SELECT ON msdb.dbo.sysjobsteps TOVC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	

Table 7-2. Microsoft SQL Database Permissions for vCenter Server (Continued)

Permission	Description
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_lock TO VC_ADMIN_ROLE	Necessary during installation or upgrade. Verifies that the provided database is not used by another connection.
GRANT VIEW SERVER STATE TO [vpxuser]	Provides access to SQL Server DMV views.
GRANT VIEW ANY DEFINITION TO [vpxuser]	Necessary for providing the user with the privileges to see metadata for SQL Server objects.

Table 7-3. Oracle Database Permissions for vCenter Server

Permission	Description
GRANT CONNECT TO VPXADMIN	Necessary for connecting to the Oracle database.
GRANT RESOURCE TO VPXADMIN	Necessary for creating a trigger, sequence, type, procedure, and so on. 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.
GRANT CREATE VIEW TO VPXADMIN	Necessary for creating a view.
GRANT CREATE SEQUENCE TO VPXADMIN	Necessary for creating a sequence.
GRANT CREATE TABLE TO VPXADMIN	Necessary for creating a table.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Necessary for creating a materialized view.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Necessary for guaranteeing that the vCenter Server database is used by a single vCenter Server instance.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Necessary during installation or upgrade for scheduling and managing the SQL jobs. This permission is not required after deployment.
GRANT SELECT ON dba_lock TO VPXADMIN	Necessary for determining existing locks on the vCenter Server database.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Necessary during upgrade for determining the required disk space. This permission is not required after deployment.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Necessary during upgrade for determining the required disk space. This permission is not required after deployment.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necessary for monitoring the free space while vCenter Server is working.
GRANT SELECT ON v_$session TO VPXADMIN	View used to determine existing locks on the vCenter Server database.

Table 7-3. Oracle Database Permissions for vCenter Server (Continued)

Permission	Description
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Necessary for granting unlimited tablespace permissions to the vCenter Server database user.
GRANT SELECT ON v_$system_event TO VPXADMIN	Necessary for checking log file switches.
GRANT SELECT ON v_$sysmetric_history TO VPXADMIN	Necessary for checking the CPU utilization.
GRANT SELECT ON v_$sysstat TO VPXADMIN	Necessary for determining the Buffer Cache Hit Ratio.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necessary for determining the tablespace utilization.
GRANT SELECT ON v_$loghist TO VPXADMIN	Necessary for checking the checkpoint frequency.

The privileges on the master database are used to monitor the vCenter Server database. so that, for example, if a certain threshold is reached, you can see an alert.

How vCenter Single Sign-On Affects Installation

Starting with version 5.1, vSphere includes a vCenter Single Sign-On service as part of the vCenter Server management infrastructure. This change affects vCenter Server installation.

Authentication with vCenter Single Sign-On makes vSphere more secure because the vSphere software components communicate with each other by using a secure token exchange mechanism, and all other users also authenticate with vCenter Single Sign-On.

Starting with vSphere 6.0, vCenter Single Sign-On is either included in an embedded deployment, or part of the Platform Services Controller. The Platform Services Controller contains all of the services that are necessary for the communication between vSphere components including vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service, and the licensing service.

The order of installation is important.

First installation

If your installation is distributed, you must install the Platform Services Controller before you install vCenter Server or deploy the vCenter Server Appliance. For an embedded deployment the correct installation order happens automatically.

Subsequent installations

For approximately up to eight vCenter Server instances, one Platform Services Controller can serve your entire vSphere environment. You can connect the new vCenter Server instances to the same Platform Services Controller. For more than approximately eight vCenter Server instances, you can install an additional Platform Services Controller for better performance. The vCenter Single Sign-On service on each Platform Services Controller synchronizes authentication data with all other instances. The precise number depends on how heavily the vCenter Server instances are being used and on other factors.

vCenter Single Sign-On Components

vCenter Single Sign-On includes the Security Token Service (STS), an administration server, and vCenter Lookup Service, as well as the VMware Directory Service (vmdir). The VMware Directory Service is also used for certificate management.

During installation, the components are deployed as part an embedded deployment, or as part of the Platform Services Controller.

STS (Security Token Service)

The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the identity source types supported byvCenter Single Sign-On. The SAML tokens allow both human users and solution users who authenticate successfully to vCenter Single Sign-On to use any vCenter service that vCenter Single Sign-On supports without authenticating again to each service.

The vCenter Single Sign-On service signs all tokens with a signing certificate, and stores the token signing certificate on disk. The certificate for the service itself is also stored on disk.

Administration server

The administration server allows users with administrator privileges to vCenter Single Sign-On to configure the vCenter Single Sign-On server and manage users and groups from the vSphere Web Client. Initially, only the user administrator@*your_domain_name* has these privileges. In vSphere 5.5 this user was administrator@vsphere.local. With vSphere 6.0, you can change the vSphere domain when you install vCenter Server or deploy the vCenter Server Appliance with a new Platform Services Controller. Do not name the domain name with your Microsoft Active Directory or OpenLDAP domain name.

VMware Directory Service (vmdir)

The VMware Directory service (vmdir) is associated with the domain you specify during installation and is included in each embedded deployment and on each Platform Services Controller. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available on port 389. The service still uses port 11711 for backward compatibility with vSphere 5.5 and earlier systems.

If your environment includes more than one instance of the Platform Services Controller, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir.

Starting with vSphere 6.0, the VMware Directory Service stores not only vCenter Single Sign-On information but also certificate information.

Identity Management Service

Handles identity sources and STS authentication requests.

Setting the vCenter Server Administrator User

The way you set the vCenter Server administrator user depends on your vCenter Single Sign-On deployment.

In vSphere versions before vSphere 5.1, vCenter Server administrators are the users that belong to the local operating system administrators group.

In vSphere 5.1.x, 5.5, and 6.0, when you install vCenter Server, you must provide the default (initial) vCenter Server administrator user or group. For deployments where vCenter Server and vCenter Single Sign-On are on the same virtual machine or physical server, you can designate the local operating system group Administrators as vCenter Server administrative users. This option is the default. This behavior is unchanged from vCenter Server 5.0.

For larger installations, where vCenter Single Sign-On is part of the Platform Services Controller and vCenter Server are deployed on different virtual machines or physical servers, you cannot preserve the same behavior as in vCenter Server 5.0. Instead, assign the vCenter Server administrator role to a user or group from an identity source that is registered in the vCenter Single Sign-On server: Active Directory, OpenLDAP, or the system identity source.

Authenticating to the vCenter Server Environment

In vCenter Server versions 5.1 and later, users authenticate through vCenter Single Sign-On.

In vCenter Server versions earlier than vCenter Server 5.1, when a user connects to vCenter Server, vCenter Server authenticates the user by validating the user against an Active Directory domain or the list of local operating system users.

The user administrator@*your_domain_name* has vCenter Single Sign-On administrator privileges by default. When logged in to the vCenter Single Sign-On server from the vSphere Web Client, the administrator@*your_domain_name* user can assign vCenter Single Sign-On administrator privileges to other users. These users might be different from the users that administer vCenter Server.

Users can log in to vCenter Server with the vSphere Web Client. Users authenticate to vCenter Single Sign-On. Users can view all the vCenter Server instances that the user has permissions on. After users connect to vCenter Server, no further authentication is required. The actions users can perform on objects depend on the user's vCenter Server permissions on those objects.

For more information about vCenter Single Sign-On, see *vSphere Security*.

How vCenter Single Sign-On Affects Log In Behavior

vCenter Single Sign-On log in behavior depends on the domain the user belongs to and the identity sources that you have added to vCenter Single Sign-On.

When a user logs in to a vCenter Server system from the vSphere Web Client, the login behavior depends on whether the user is in the default domain, that is, the domain that is set as the default identity source.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

vCenter Single Sign-On does not propagate permissions to authenticate that result from nested groups from dissimilar identity sources. For example, if you add the Domain Administrators group to the Local Administrators group, the permissions are not propagated because Local OS and Active Directory are separate identity sources.

After installation on a Windows system, the user administrator@*your_domain_name* has administrator privileges to both the vCenter Single Sign-On server and the vCenter Server system.

After you deploy the vCenter Server Appliance, the user administrator@*your_domain_name* has administrator privileges to both the vCenter Single Sign-On server and the vCenter Server system.

Identity Sources for vCenter Server with vCenter Single Sign-On

You can use identity sources to attach one or more domains to vCenter Single Sign-On. A domain is a repository for users and groups that the vCenter Single Sign-On server can use for user authentication.

An identity source is a collection of user and group data. The user and group data is stored in Active Directory, OpenLDAP, or locally to the operating system of the machine where vCenter Single Sign-On is installed.

After installation, every instance of vCenter Single Sign-On has the identity source *your_domain_name*, for example vsphere.local. This identity source is internal to vCenter Single Sign-On. A vCenter Single Sign-On administrator can add identity sources, set the default identity source, and create users and groups in the vsphere.local identity source.

Types of Identity Sources

vCenter Server versions earlier than version 5.1 supported Active Directory and local operating system users as user repositories. As a result, local operating system users could always authenticate to the vCenter Server system. vCenter Server version 5.1 and version 5.5 uses vCenter Single Sign-On for authentication. See the vSphere 5.1 documentation for a list of supported identity sources with vCenter Single Sign-On 5.1. vCenter Single Sign-On 5.5 supports the following types of user repositories as identity sources, but supports only one default identity source.

- Active Directory versions 2003 and later. Shown as **Active Directory (Integrated Windows Authentication)** in the vSphere Web Client. vCenter Single Sign-On allows you to specify a single Active Directory domain as an identity source. The domain can have child domains or be a forest root domain. VMware KB article 2064250 discusses Microsoft Active Directory Trusts supported with vCenter Single Sign-On.

- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources. This identity source type is included for compatibility with the vCenter Single Sign-On service included with vSphere 5.1. Shown as **Active Directory as an LDAP Server** in the vSphere Web Client.

- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources. Shown as **OpenLDAP** in the vSphere Web Client.

- Local operating system users. Local operating system users are local to the operating system where the vCenter Single Sign-On server is running. The local operating system identity source exists only in basic vCenter Single Sign-On server deployments and is not available in deployments with multiple vCenter Single Sign-On instances. Only one local operating system identity source is allowed. Shown as **localos** in the vSphere Web Client.

  NOTE Do not use local operating system users if the Platform Services Controller is on a different machine than the vCenter Server system. Using local operating system users might make sense in an embedded deployment but is not recommended.

- vCenter Single Sign-On system users. Exactly one system identity source named vsphere.local is created when you install vCenter Single Sign-On. Shown as **vsphere.local** in the vSphere Web Client.

NOTE At any time, only one default domain exists. If a user from a non-default domain logs in, that user must add the domain name (*DOMAIN*\user) to authenticate successfully.

vCenter Single Sign-On identity sources are managed by vCenter Single Sign-On administrator users.

You can add identity sources to a vCenter Single Sign-On server instance. Remote identity sources are limited to Active Directory and OpenLDAP server implementations.

For more information about vCenter Single Sign-On, see *vSphere Security*.

Synchronizing Clocks on the vSphere Network

Make sure that components on the vSphere network have their clocks synchronized. If the clocks on the machines in your vSphere network are not synchronized, SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

Make sure any Windows host machine on which a vCenter component runs is synchronized with the NTP server. See the Knowledge Base article Timekeeping best practices for Windows, including NTP.

Synchronize ESXi Clocks with a Network Time Server

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

Procedure

1. Start the vSphere Client, and connect to the ESXi host.
2. On the **Configuration** tab, click **Time Configuration**.
3. Click **Properties**, and click **Options**.
4. Select **NTP Settings**.
5. Click **Add**.
6. In the Add NTP Server dialog box, enter the IP address or fully qualified domain name of the NTP server to synchronize with.
7. Click **OK**.

   The host time synchronizes with the NTP server.

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.

IMPORTANT If the vCenter Server service is running under the Microsoft Windows built-in system account, when using Microsoft SQL Server, vCenter Server 6.0 supports only DSNs with SQL Server authentication.

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 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 and the account must be granted the **Log on as a service** privilege.

Installing vCenter Server on IPv6 Machines

Starting with vSphere 6.0, vCenter Server supports connection between vCenter Server and vCenter Server components by either IPv4 or IPv6 addresses.

Mixed IPv4 and IPv6 environment is not supported. When you install vCenter Server in an IPv6 environment, use the fully qualified domain name (FQDN) or host name of the machine on which you install vCenter Server. For pure IPv4 environment, the best practice is to use the fully qualified domain name (FQDN) or host name of the machine on which you install vCenter Server, because the IP address can change if assigned by DHCP.

Running the vCenter Server Installer from a Network Drive

You can run the vCenter Server installer 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

When you install vCenter Server with an embedded or external Platform Services Controller, the installation wizard prompts you for the installation information.

Required Information for Installing vCenter Server with an Embedded Platform Services Controller

The vCenter Server installation wizard prompts you for the installation information. It is a best practice to keep a record of the values that you entered in case you must reinstall the product.

You can use this worksheet to record the information that you need for the installation of vCenter Server with an embedded Platform Services Controller.

Table 7-4. Information Required for Installing vCenter Server with an Embedded Platform Services Controller

Required Information		Default	Your Entry
System name of the local system. A system name to use for managing the local system. The system name must be an FQDN. If a DSN is not available, provide a static IP address.			
New vCenter Single Sign-On domain.	Domain name	vsphere.local	
	User name	administrator	You cannot change the default user name during installation.
	Password for the vCenter Single Sign-On administrator account. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, such as ampersand (&), hash key (#), and percent sign (%).		

Table 7-4. Information Required for Installing vCenter Server with an Embedded Platform Services Controller (Continued)

Required Information			Default	Your Entry
	Site name. A name for the vCenter Single Sign-On site.			
Join a vCenter Single Sign-On domain.	Platform Services Controller FQDN or IP address.			
	HTTPS port to communicate with an existing vCenter Single Sign-On domain		443	
	Password for the vCenter Single Sign-On administrator account.			
	Join an existing site or create a new site.	Name of the site to join or name of the new site.		
vCenter Server Service account information. Can be the Windows system account or a user-specified account.	Account user name Required if you use a user service account.			
	Account password Required if you use a user service account.			
Data source name (DSN). Required if you plan to use an existing external database. Not required if you plan to use the bundled PostrgreSQL database. Leading and trailing spaces are not supported. Remove spaces from the beginning or end of the DSN.				
Database user name.	Required if you plan to use an existing database. Not required if you plan to use the bundled PostgreSQL database. Non-ASCII characters are not supported.			
Database password.				
HTTP port.			80	
HTTPS port.			443	
Syslog Service port.			514	
Syslog Service TLS port.			1514	
Secure Token Service port.			7444	
Auto Deploy Management port.			6502	
Auto Deploy Service port.			6501	
ESXi Dump Collector port.			6500	
ESXi Heartbeat port.			902	

Table 7-4. Information Required for Installing vCenter Server with an Embedded Platform Services Controller (Continued)

Required Information	Default	Your Entry
vSphere Web Client port.	9443	
Destination folder. - The folder in which to install vCenter Server. - The folder in which to store data for vCenter Server with an embedded Platform Services Controller. The installation paths cannot contain non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).	- The default installation folder is `C:\Program Files\VMware`. - The default folder for data storage is `C:\ProgramData\VMware`.	

Required Information for Installing a Platform Services Controller

When you install vCenter Server with an external Platform Services Controller, the Platform Services Controller installation wizard prompts you for the installation information. It is a best practice to keep a record of the values that you entered in case you must reinstall the product.

You can use this worksheet to record the information that you need for the installation of an external Platform Services Controller.

Table 7-5. Information Required for Installing an External Platform Services Controller

Required Information		Default	Your Entry
System name of the local system. A system name to use for managing the local system. The system name must be an FQDN. If a DSN is not available, provide a static IP address.			
New vCenter Single Sign-On domain.	Domain name	vsphere.local	
	User name	administrator	You cannot change the default user name during installation.
	Password for the vCenter Single Sign-On administrator account. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: - Must contain at least one uppercase letter. - Must contain at least one lowercase letter. - Must contain at least one number. - Must contain at least one special character, such as ampersand (&), hash key (#), and percent sign (%).		
	Site name. A name for the vCenter Single Sign-On site.		
Join a vCenter Single Sign-On domain.	Platform Services Controller FQDN or IP address		
	HTTPS port to communicate with an existing vCenter Single Sign-On domain	443	

Table 7-5. Information Required for Installing an External Platform Services Controller (Continued)

Required Information			Default	Your Entry
	Password for the vCenter Single Sign-On administrator account.			
	Join an existing site or create a new site	Name of the site to join or name of the new site.		
HTTP port.			80	
HTTPS port.			443	
Syslog Service port.			514	
Syslog Service TLS port.			1514	
Secure Token Service port.			7444	
Destination folder. ■ The folder in which to install the Platform Services Controller. ■ The folder in which to store data for the Platform Services Controller. The installation paths cannot contain non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).			■ The default installation folder is `C:\Program Files\VMware`. ■ The default folder for data storage is `C:\ProgramData\VMware`.	

Required Information for Installing vCenter Server

When you install vCenter Server with an external Platform Services Controller, the vCenter Server installation wizard prompts you for the installation information. It is a best practice to keep a record of the values that you entered in case you have to reinstall the product.

You can use this worksheet to record the information that you need for the installation of vCenter Server with an external Platform Services Controller.

Table 7-6. Information Required for Installing vCenter Server with an External Platform Services Controller

Required Information		Default value	Your Entry
System name of the local system. A system name to use for managing the local system. The system name must be an FQDN. If a DSN is not available, provide a static IP address.			
Single Sign-On information.	Platform Services Controller FQDN or IP address.		
	Single Sign-On HTTPS port.	443	
	Single Sign-On user name.		
	Single Sign-On user password.		
vCenter Server Service account information. Can be the Windows system account or a user-specified account.	Account user name Required if you use a user service account.		
	Account password Required if you use a user service account.		

Table 7-6. Information Required for Installing vCenter Server with an External Platform Services Controller (Continued)

Required Information		Default value	Your Entry
Data source name (DSN). Required if you use an existing external database. Not required if you are using the bundled PostgreSQL database. Leading and trailing spaces are not supported. Remove spaces from the beginning or end of the DSN.			
Database user name.	Required if you plan to use an existing database. Not required if you plan to use the bundled PostgreSQL database. Non-ASCII characters are not supported.		
Database password.			
HTTP port.		80	
HTTPS port.		443	
Syslog Service port.		514	
Syslog Service TLS port.		1514	
Auto Deploy Management port.		6502	
Auto Deploy Service port.		6501	
ESXi Dump Collector port.		6500	
ESXi Heartbeat port.		902	
vSphere Web Client port.		9443	
Destination folders. ■ The folder in which to install vCenter Server. ■ The folder in which to store data for vCenter Server with an external Platform Services Controller. The installation paths cannot contain non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).		■ The default installation folder is `C:\Program Files\VMware`. ■ The default folder for data storage is `C:\ProgramData\VMware`.	

Required Information for Deploying the vCenter Server Appliance

When you deploy the vCenter Server Appliance with an embedded or external Platform Services Controller, the installation wizard prompts you for the deployment information.

Required Information for Deploying the vCenter Server Appliance with an Embedded Platform Services Controller

The vCenter Server Appliance deployment wizard prompts you for the deployment information. It is a best practice to keep a record of the values that you entered in case you must reinstall the product.

You can use this worksheet to record the information that you need for deploying a vCenter Server Appliance with an embedded Platform Services Controller.

Table 7-7. Information Required for Deploying vCenter Server Appliance with an Embedded Platform Services Controller

Required Information		Default	Your Entry
FQDN or IP of the ESXi host on which you deploy the vCenter Server Appliance			
ESXi host user name			
ESXi host password			
vCenter Server Appliance name		Example: Sample-Appliance-Name	
Password of the root user of the vCenter Server Appliance operating system. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!).			
New Single Sign-On domain.	Domain name	vsphere.local	
	User name	administrator	You cannot change the default user name during installation.
	Password for the vCenter Single Sign-On administrator account. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, such as ampersand (&), hash key (#), and percent sign (%).		
	Site name. A name for the vCenter Single Sign-On site.		
Join a Single Sign-On domain.	Platform Services Controller FQDN or IP address.		
	Password for the vCenter Single Sign-On administrator account.		
	Port number	443	
	Site name		

Table 7-7. Information Required for Deploying vCenter Server Appliance with an Embedded Platform Services Controller (Continued)

Required Information		Default	Your Entry
vCenter Server Appliance size. The options vary depending on the size of your vSphere environment: ■ Tiny (up to 10 hosts, 100 virtual machines) ■ Small (up to 100 hosts, 1,000 virtual machines) ■ Medium (up to 400 hosts, 4,000 virtual machines) ■ Large (up to 1,000 hosts, 10,000 virtual machines)		Tiny (up to 10 hosts, 100 virtual machines	
Name of the datastore on which the vCenter Server Appliance is deployed.			
Enable or disable Thin Disk Mode.		Disabled by default	
Oracle database server.	Required if you plan to use an existing Oracle database. Not required if you plan to use the bundled PostgreSQL database. Non-ASCII characters are not supported.		
Oracle database port.			
Oracle database instance name.			
Database user name.			
Database password.			
Network name.			
IP address allocation. Can be either IPv4 or IPv6.		IPv4	
Network type. Can be either DHCP or static for IPv4; and DHCP or static for IPv6.		DHCP	
IPv4 address assigned by DHCP settings.	FQDN If there is no enabled DNS in your environment, leave the FQDN text box blank.		
	Enable or disable SSH.	Disabled by default	
IPv4 static assignment settings.	Network address.		
	System name (FQDN or IP address). A system name to use for managing the local system. The system name must be FQDN. If DNS is not available, provide a static IP address.		
	Subnet mask.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
IPv6 address assigned by DHCP settings	FQDN If there is no enabled DNS in your environment, leave the FQDN text box blank.		
	Enable or disable SSH	Disabled by default	

Table 7-7. Information Required for Deploying vCenter Server Appliance with an Embedded Platform Services Controller (Continued)

Required Information		Default	Your Entry
IPv6 static assignment settings.	FQDN		
	Network address.		
	Network prefix.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
Time synchronization settings. You can synchronize the time of the appliance either with the time of the ESXi host, or use NTP servers.	Names of the NTP servers, separated by commas. Required to use NTP servers for time synchronization.		

Required Information for Deploying the Platform Services Controller Appliance

The Platform Services Controller deployment wizard prompts you for the deployment information. It is a best practice to keep a record of the values that you entered in case you must reinstall the product.

You can use this worksheet to record the information that you need for deploying an external Platform Services Controller.

Table 7-8. Information Required for Deploying an External Platform Services Controller

Required Information		Default Value	Your Entry
FQDN or IP of the ESXi host on which you deploy the Platform Services Controller appliance.			
ESXi host user name			
ESXi host password			
Platform Services Controller appliance name		Example: Sample-Appliance-Name	
Password of the root user of the vCenter Server Appliance operating system. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!).			
New Single Sign-On domain.	Domain name	vsphere.local	

Table 7-8. Information Required for Deploying an External Platform Services Controller (Continued)

Required Information		Default Value	Your Entry
	Password for the vCenter Single Sign-On administrator account. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, such as ampersand (&), hash key (#), and percent sign (%).		
	Site name. A name for the vCenter Single Sign-On site.		
Join a Single Sign-On domain.	Platform Services Controller FQDN or IP address		
	Password for the vCenter Single Sign-On administrator account.		
	Port number	443	
	Site name		
Platform Services Controller appliance size.		Platform Services Controller	You cannot change the default option. The virtual appliance that you deploy will be with 2 CPUs and 2 GB memory.
Name of the datastore on which the Platform Services Controller appliance is deployed.			
Enable or disable Thin Disk Mode.		Disabled by default	
Network name.			
IP address allocation. Can be either IPv4 or IPv6.		IPv4	
Network type. Can be either DHCP or static for IPv4; and DHCP or static for IPv6.		DHCP	
IPv4 address assigned by DHCP settings	FQDN If there is no enabled DDNS in your environment, leave the FQDN text box blank.		
	Enable or disable SSH.	Disabled by default	
IPv4 static assignment settings.	Network address.		

Table 7-8. Information Required for Deploying an External Platform Services Controller (Continued)

Required Information		Default Value	Your Entry
	System name (FQDN or IP address). A system name to use for managing the local system. The system name must be FQDN. If DNS is not available, provide a static IP address.		
	Subnet mask.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
IPv6 address assigned by DHCP settings	FQDN If you have notenabled DNS, leave the FQDN text box blank.		
	Enable or disable SSH	Disabled by default	
IPv6 static assignment settings.	FQDN		
	Network address.		
	Network prefix.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
Time synchronization settings. You can synchronize the time of the appliance either with the time of the ESXi host, or use NTP servers.	Names of the NTP servers, separated by commas. Required to use NTP servers for time synchronization.		

Required Information for Deploying the vCenter Server Appliance

The vCenter Server Appliance deployment wizard prompts you for the deployment information. It is a best practice to keep a record of the values that you entered in case you must reinstall the product.

You can use this worksheet to record the information that you need for deploying a vCenter Server Appliance with an external Platform Services Controller.

Table 7-9. Information Required for Deploying the vCenter Server Appliance

Required Information	Default Value	Your Entry
FQDN or IP of the ESXi host on which you deploy the vCenter Server Appliance		
ESXi host user name		
ESXi host password		
vCenter Server Appliance name	Example: Sample-Appliance-Name	

Table 7-9. Information Required for Deploying the vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
Password of the root user of the vCenter Server Appliance operating system. The password must be at least 8 characters, but no more than 20 characters in length. The password must conform to the following requirements: ■ Must contain at least one uppercase letter. ■ Must contain at least one lowercase letter. ■ Must contain at least one number. ■ Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!).			
Platform Services Controller FQDN or IP address. You must provide the FQDN or IP address of a Platform Services Controller that you already installed or deployed .			
vCenter Single Sign-On administrator password.			
vCenter Single Sign-On HTTPS port.		443	
vCenter Server Appliance size. The options vary depending on the size of your vSphere environment. ■ Tiny (up to 10 hosts, 100 virtual machines) ■ Small (up to 100 hosts, 1,000 virtual machines) ■ Medium (up to 400 hosts, 4,000 virtual machines) ■ Large (up to 1,000 hosts, 10,000 virtual machines)		Tiny (up to 10 hosts, 100 virtual machines)	
Name of the datastore on which the vCenter Server Appliance is deployed.			
Enable or disable thin disk mode.		Disabled by default	
Oracle database server.	Required only if you plan to use an existing Oracle database. Not required if you are using the bundled PostgreSQL database. Non-ASCII characters are not supported.		
Oracle database port.			
Oracle database instance name.			
Database user name.			
Database password.			
Network name.			
IP address allocation. Can be either IPv4 or IPv6.		IPv4	
Network type. Can be either DHCP or static for IPv4; and DHCP or static for IPv6.		DHCP	
IPv4 address assigned by DHCP settings	FQDN If there is no enabled DNS in your environment, leave the FQDN text box blank.		
	Enable or disable SSH.	Disabled by default	
IPv4 static assignment settings.	Network address.		

Table 7-9. Information Required for Deploying the vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
	System name (FQDN or IP address). A system name to use for managing the local system. The system name must be FQDN. If DNS is not available, provide a static IP address.		
	Subnet mask.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
IPv6 address assigned by DHCP settings	FQDN If there is no enabled DNS in your environment, leave the FQDN text box blank.		
	Enable or disable SSH	Disabled by default	
IPv6 static assignment settings.	FQDN		
	Network address.		
	Network prefix.		
	Network gateway.		
	Network DNS servers separated by commas.		
	Enable or disable SSH.	Disabled by default	
Time synchronization settings. You can synchronize the time of the appliance either with the time of the ESXi host, or use NTP servers.	Names of the NTP servers, separated by commas. Required to use NTP servers for time synchronization.		

Installing vCenter Server on a Windows Virtual Machine or Physical Server

8

You can install vCenter Server on a Microsoft Windows virtual machine or physical server to manage your vSphere environment.

Before you install vCenter Server, download the ISO file and mount it to the Windows host machine from which you want to perform the installation, and then start the installation wizard.

For information about the vCenter Server requirements, see "vCenter Server for Windows Requirements," on page 29.

For information about the inputs that are required during the installation of vCenter Server, see "Required Information for Installing vCenter Server," on page 210.

After you install vCenter Server, only the user administrator@*your_domain_name* has the privileges to log in to the vCenter Server system.

The administrator@*your_domain_name* user can perform the following tasks:

- Add an identity source in which additional users and groups are defined in vCenter Single Sign-On.
- Assign roles to users and groups to give them privileges.

For information about adding identity sources and giving permissions to the users and groups, see *vSphere Security*.

This chapter includes the following topics:

Download the vCenter Server for Windows Installer

Download the `.iso` installer for vCenter Server for Windows and the associated vCenter Server components and support tools.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1. Download the vCenter Server installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

   vCenter Server is part of VMware vCloud Suite and VMware vSphere, listed under Datacenter & Cloud Infrastructure.

2. Confirm that the md5sum is correct.

   See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

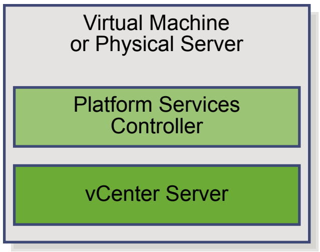
3. Mount the ISO image to the Windows virtual machine or physical server on which you want to install vCenter Server for Windows.

Install vCenter Server with an Embedded Platform Services Controller

You can deploy vCenter Server, the vCenter Server components, and the Platform Services Controller on one virtual machine or physical server.

You cannot change the deployment model to vCenter Server with an external Platform Services Controller after the installation completes.

Figure 8-1. vCenter Server with an Embedded Platform Services Controller



IMPORTANT Concurrent installations of vCenter Server instances with embedded Platform Services Controllers are not supported. You must install the vCenter Server instances with embedded Platform Services Controllers in a sequence.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server installer.
- If you want to use the vSphere Web Client on the host machine on which you install vCenter Server, verify that Adobe Flash Player version 11.9 or later is installed on the system.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server for Windows** and click **Install**.
3. Follow the prompts of the installation wizard to review the welcome page and accept the license agreement.
4. Select **vCenter Server and Embedded Platform Services Controller**, and click **Next**.

5 Enter the system network name, preferably an FQDN, and click **Next**.

You can also enter an IP address. If you enter an IP address, provide a static IP address.

IMPORTANT Make sure the FQDN or IP address that you provide does not change. The system name cannot be changed after deployment. If the system name changes, you must uninstall vCenter Server and install it again.

6 Create a new vCenter Single Sign-On domain or join an existing domain.

IMPORTANT Although you can select to join a vCenter Single Sign-On domain, you should consider vCenter Server with an embedded Platform Services Controller as a standalone installation and do not use it for replication of infrastructure data.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On server. a Enter the domain name, for example **`vsphere.local`**. b Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*your_domain_name*, where *your_domain_name* is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and to vCenter Server as adminstrator@*your_domain_name*. c Enter the site name for vCenter Single Sign-On. The site name is important if you are using vCenter Single Sign-On in multiple locations. The site name must contain alphanumeric characters. Choose your own name for the vCenter Single Sign-On site. You cannot change the name after installation. Non-ASCII or high-ASCII characters are not supported in site names. Your site name must include alphanumeric characters and a comma (,), period (.), question mark (?), dash (-), underscore (_), plus sign (+) or equals sign (=).
Join a Single Sign-On domain in an existing Platform Services Controller	Joins a new vCenter Single Sign-On server to a vCenter Single Sign-On domain in an existing Platform Services Controller. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. a Type the fully qualified domain name (FQDN) or IP address of the Platform Services Controller that contains the vCenter Single Sign-On server to join. b Type the HTTPS port to use for communication with the Platform Services Controller. c Type the password of the vCenter Single Sign-On administrator account. d Click **Next**. e Approve the certificate provided by the remote machine, and you must select whether to create or join an existing vCenter Single Sign-On site. f Select whether to create or join an existing vCenter Single Sign-On site.

7 Click **Next**.

8 Select the vCenter Server service account and click **Next**.

Option	Description
Use Windows Local System Account	The vCenter Server service runs in the Windows Local System account. This option prevents you from connecting to an external database by using Windows integrated authentication.
Specify a user service account	The vCenter Server service runs in an administrative user account with a user name and password that you provide.

IMPORTANT The user credentials that you provide must be of a user who is in the local administrator group and who has the **Log on as a service** privilege.

9 Select the type of database that you want to use and click **Next**.

Option	Description
Use an embedded database (vPostgres)	vCenter Server uses the embedded PostgreSQL database. This database is suitable for small scale deployments.
Use an external database	vCenter Server uses an existing external database. a Select your database from the list of available DSNs. b Type the user name and the password for the DSN. If your database uses Windows NT authentication, the user name and password text boxes are disabled.

10 For each component, accept the default port numbers, or if another service is using the defaults, enter alternative ports, and click **Next**.

Make sure that ports 80 and 443 are free and dedicated, so that vCenter Single Sign-On can use these ports. Otherwise, use custom ports during installation.

11 (Optional) Change the default destination folders and click **Next**.

IMPORTANT Do not use folders that end with an exclamation mark (!).

12 Review the summary of the installation settings and click **Install**.

13 (Optional) Click **Launch vSphere Web Client** to start the vSphere Web Client and log in to vCenter Server.

14 After the installation completes, click **Finish**.

vCenter Server, the vCenter Server components, and the Platform Services Controller are installed.

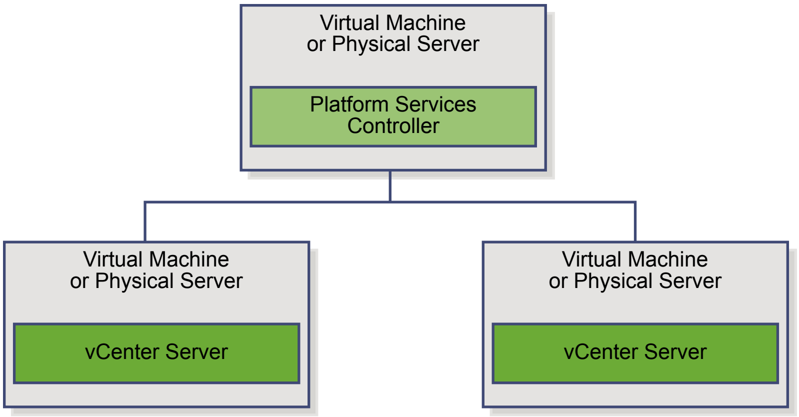
Installing vCenter Server with an External Platform Services Controller

You can install vCenter Server and the Platform Services Controller on different virtual machines or physical servers.

You can separate the Platform Services Controller and vCenter Server and have them installed on different virtual machines or physical servers. First install the Platform Services Controller, then install vCenter Server and the vCenter Server components on another virtual or physical machine, and connect vCenter Server to the Platform Services Controller. You can connect many vCenter Server instances to one Platform Services Controller.

IMPORTANT Concurrent installations of vCenter Server instances and Platform Services Controllers are not supported. You must install the Platform Services Controllers and vCenter Server instances in a sequence.

Figure 8-2. vCenter Server with an External Platform Services Controller


Virtual Machine or Physical Server
Platform Services Controller
Virtual Machine or Physical Server
vCenter Server
Virtual Machine or Physical Server
vCenter Server

You cannot change the deployment model to vCenter Server with an embedded Platform Services Controller after the installation completes.

IMPORTANT Before installing vCenter Server with an external Platform Services Controller, synchronize the clocks on the vSphere network. Time skew on the virtual machines or physical servers on which you install the Platform Services Controller and vCenter Server might cause deployment failure. For instructions about synchronizing the clocks on your vSphere network, see "Synchronizing Clocks on the vSphere Network," on page 209.

Install a Platform Services Controller on a Windows Machine

To install vCenter Server with an external Platform Services Controller, first install a Platform Services Controller for Windows. The Platform Services Controller contains the common services, such as vCenter Single Sign-On and the License service, which can be shared across several vCenter Server instances.

You can install many Platform Services Controllers and join them to the same vCenter Single Sign-On domain. Concurrent installations of Platform Services Controllers are not supported. You must install the Platform Services Controllers in a sequence.

IMPORTANT If you want to replace the VMCA-signed certificate with a CA-signed certificate, install the Platform Services Controller first, and then include VMCA in the certificate chain and generate new certificates from VMCA that are signed by the whole chain. You can then install vCenter Server. For information about managing vCenter Server certificates, see the *vSphere Security* documentation.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server installer.
- If you want to use the vSphere Web Client on the host machine on which you install vCenter Server, verify that Adobe Flash Player version 11.9 or later is installed on the system.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server for Windows** and click **Install**.
3. Follow the prompts of the installation wizard to review the welcome page and accept the license agreement.
4. Select **Platform Services Controller** and click **Next**.

5 Enter the system name, preferably an FQDN, and click **Next**.

You can also enter an IP address. If you enter an IP address, provide a static IP address.

IMPORTANT When you provide an FQDN or an IP address as the system name of the Platform Services Controller, make sure that the FQDN or IP address does not change. If the FQDN or IP address of the host machine changes, you have to reinstall the Platform Services Controller and the vCenter Server instances registered with it. The FQDN or IP address of the Platform Services Controller is used to generate an SSL certificate for the Platform Services Controller host machine.

6 Create a new vCenter Single Sign-On domain or join an existing domain.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On server. a Enter the domain name, for example `vsphere.local`. b Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*your_domain_name*, where *your_domain_name* is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and to vCenter Server as adminstrator@*your_domain_name*. c Enter the site name for vCenter Single Sign-On. The site name is important if you are using vCenter Single Sign-On in multiple locations. The site name must contain alphanumeric characters. Choose your own name for the vCenter Single Sign-On site. You cannot change the name after installation. Non-ASCII or high-ASCII characters are not supported in site names. Your site name must include alphanumeric characters and a comma (,), period (.), question mark (?), dash (-), underscore (_), plus sign (+) or equals sign (=).
Join a Single Sign-On domain in an existing Platform Services Controller	Joins a new vCenter Single Sign-On server to a vCenter Single Sign-On domain in an existing Platform Services Controller. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. a Type the fully qualified domain name (FQDN) or IP address of the Platform Services Controller that contains the vCenter Single Sign-On server to join. b Type the HTTPS port to use for communication with the Platform Services Controller. c Type the password of the vCenter Single Sign-On administrator account. d Click **Next**. e Approve the certificate provided by the remote machine, and you must select whether to create or join an existing vCenter Single Sign-On site. f Select whether to create or join an existing vCenter Single Sign-On site.

When you select to join an existing vCenter Single Sign-On domain, you enable the Enhanced Linked Mode feature. Your Platform Services Controller will replicate infrastructure data with the joined vCenter Single Sign-On server.

7 Click **Next**.

8 For each component, accept the default port numbers, or if another service is using the defaults, enter alternative ports, and click **Next**.

Make sure that ports 80 and 443 are free and dedicated, so that vCenter Single Sign-On can use these ports. Otherwise, use custom ports during installation.

9 (Optional) Change the default destination folders and click **Next**.

IMPORTANT Do not use folders that end with an exclamation mark (!).

10 Review the summary of the installation settings and click **Install**.

11 After the installation completes, click **Finish**.

The Platform Services Controller is installed.

What to do next

Install vCenter Server on another Windows virtual machine or physical server and register vCenter Server and the vCenter Server components to the Platform Services Controller.

Install vCenter Server and the vCenter Server Components

After you install a Platform Services Controller on a Windows host machine, or deploy a Platform Services Controller appliance, you can install vCenter Server and the vCenter Server components and connect the vCenter Server instance to the deployed Platform Services Controller.

Concurrent installations of vCenter Server instances are not supported. If you want to install many vCenter Server instances and register them with the same Platform Services Controller or Platform Services Controller appliance, install the vCenter Server instances one by one in a sequence.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server installer.
- If you want to use the vSphere Web Client on the host machine on which you install vCenter Server, verify that Adobe Flash Player version 11.9 or later is installed on the system.

Procedure

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

2 Select **vCenter Server for Windows** and click **Install**.

3 Follow the prompts of the installation wizard to review the welcome page and accept the license agreement.

4 Select **vCenter Server** and click **Next**.

5 Enter the system network name, preferably a static IP address, and click **Next**.

IMPORTANT The name that you type is encoded in the SSL certificate of the system. The components communicate with each other by using this name. The system name must be either a static IP address or a fully qualified domain name (FQDN). Make sure that the system name does not change. You cannot change the system name after the installation completes.

6 Provide the system name of the Platform Services Controller that you already installed or deployed, the HTTPS port to use for communication with the vCenter Single Sign-On server, as well as the vCenter Single Sign-On password, and click **Next**.

IMPORTANT Make sure that you use either the IP address or the FQDN that you provided during the installation of the Platform Services Controller. If you provided the FQDN as a system name of the Platform Services Controller, you cannot use an IP address, and the reverse. When a service from vCenter Server connects to a service running in the Platform Services Controller, the certificate is verified. If the IP address or FQDN changes, the verification fails and vCenter Server cannot connect to the Platform Services Controller.

7 Approve the certificate provided by the remote machine.

8 Select the vCenter Server service account and click **Next**.

Option	Description
Use Windows Local System Account	The vCenter Server service runs in the Windows Local System account. This option prevents you from connecting to an external database by using Windows integrated authentication.
Specify a user service account	The vCenter Server service runs in an administrative user account with a user name and password that you provide.

IMPORTANT The user credentials that you provide must be of a user who is in the local administrator group and who has the **Log on as a service** privilege.

9 Select the type of database that you want to use and click **Next**.

Option	Description
Use an embedded database (vPostgres)	vCenter Server uses the embedded PostgreSQL database. This database is suitable for small scale deployments.
Use an external database	vCenter Server uses an existing external database. a Select your database from the list of available DSNs. b Type the user name and the password for the DSN. If your database uses Windows NT authentication, the user name and password text boxes are disabled.

10 For each component, accept the default port numbers, or if another service is using the defaults, enter alternative ports, and click **Next**.

11 (Optional) Change the default destination folders and click **Next**.

IMPORTANT Do not use folders that end with an exclamation mark (!).

12 Review the summary of the installation settings and click **Install**.

13 (Optional) Click **Launch vSphere Web Client** to start the vSphere Web Client and log in to vCenter Server.

14 After the installation completes, click **Finish**.

vCenter Server is installed in evaluation mode. You can activate vCenter Server by using the vSphere Web Client. For information about activating vCenter Server, see *vCenter Server and Host Management*.

Installing vCenter Server in an Environment with Multiple NICs

If you want to install vCenter Server with an externalPlatform Services Controller in an environment with multiple NICs, you must keep a record of the IP addresses or FQDNs that you use as system network names.

For example, if you want to install a Platform Services Controller on one virtual machine and vCenter Server on another virtual machine and each virtual machine has two NICs, you can use the following workflow:

1 Install a Platform Services Controller one of the virtual machines and use one of its IP addresses or FQDNs as a system network name.

2 On the other virtual machine, start the installation of vCenter Server and use one of its IP addresses or FQDNs as a system network name.

3 When prompted to provide the system network name of the Platform Services Controller, enter the IP address or FQDN that you entered during the installation of the Platform Services Controller.

If you enter the other IP address or FQDN of the Platform Services Controller, you receive an error message.

4 After the installation completes, you can log in to the vSphere Web Client by using either of the NIC IP addresses or FQDNs of vCenter Server.

Deploying the vCenter Server Appliance 9

As an alternative to installing vCenter Server on a Windows virtual machine or physical server, you can deploy the vCenter Server Appliance.

Before you deploy the vCenter Server Appliance, download the ISO file and mount it to the Windows host machine from which you want to perform the deployment. Install the Client Integration Plug-In and then start the installation wizard.

For information about the vCenter Server Appliance requirements, see "vCenter Server Appliance Requirements," on page 31.

For information about the inputs that are required during the deployment of the vCenter Server Appliance, see "Required Information for Deploying the vCenter Server Appliance," on page 214.

The vCenter Server Appliance has the following default user names:

- root with the operating system password that you enter while deploying the virtual appliance.
- administrator@*your_domain_name* with the vCenter Single Sign-On password that you enter while deploying the virtual appliance.

  After you deploy the vCenter Server Appliance, only the administrator@*your_domain_name* user has the privileges to log in to the vCenter Server system.

  The administrator@*your_domain_name* user can proceed as follows:

  - Add an identity source in which additional users and groups are defined to vCenter Single Sign-On.
  - Give permissions to the users and groups.

  For information about adding identity sources and giving permissions to the users and groups, see *vSphere Security*.

Version 6.0 of the vCenter Server Appliance is deployed with virtual hardware version 8, which supports 32 virtual CPUs per virtual machine in ESXi. Depending on the hosts that you will manage with the vCenter Server Appliance, you might want to upgrade the ESXi hosts and update the hardware version of the vCenter Server Appliance to support more virtual CPUs:

- ESXi 5.5.x supports up to virtual hardware version 10 with up to 64 virtual CPUs per virtual machine.
- ESXi 6.0 supports up to virtual hardware version 11 with up to 128 virtual CPUs per virtual machine.

Important You cannot deploy the vCenter Server Appliance by using the vSphere Client or the vSphere Web Client. During the deployment of the vCenter Server Appliance you must provide various inputs, such as operating system and vCenter Single Sign-On passwords. If you try to deploy the appliance by using the vSphere Client or the vSphere Web Client, you are not prompted to provide such inputs and the deployment fails.

For information about upgrading the vCenter Server Appliance, see *vSphere Upgrade*.

For inventory and other configuration limits in the vCenter Server Appliance, see the *Configuration Maximums* documentation.

For information about configuring the vCenter Server Appliance, see *vCenter Server Appliance Configuration*.

IMPORTANT vCenter Server 6.0 supports connection between vCenter Server and vCenter Server components by either IPv4 or IPv6 addresses. Mixed IPv4 and IPv6 environment is not supported. If you want to set up the vCenter Server Appliance to use an IPv6 address allocation, make sure to use the fully qualified domain name (FQDN) or host name of the appliance. In an IPv4 environment, the best practice is to use the FQDN or host name of the appliance, because the IP address can change if assigned by DHCP.

This chapter includes the following topics:

Download the vCenter Server Appliance Installer

Download the `.iso` installer for the vCenter Server Appliance and Client Integration Plug-in.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1 Download the vCenter Server Appliance installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

2 Confirm that the md5sum is correct.

  See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

3 Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Client Integration Plug-In to deploy or upgrade the vCenter Server Appliance.

  If you are using a Windows virtual machine, you can configure the ISO image as a datastore ISO file for the CD/DVD drive of the virtual machine by using the vSphere Web Client. See *vSphere Virtual Machine Administration*.

Install the Client Integration Plug-In

You must install the Client Integration Plug-in before you deploy or upgrade the vCenter Server Appliance.

Prerequisites

Verify that the `.iso` file for vCenter Server Appliance is downloaded and mounted.

Procedure

1 In the software installer directory, navigate to the `vcsa` directory and double-click `VMware-ClientIntegrationPlugin-6.0.0.exe`.

  The Client Integration Plug-in installation wizard appears.

2 On the Welcome page, click **Next**.

3 Read and accept the terms in the End-User License Agreement and click **Next**.

4 (Optional) Change the default path to the Client Integration Plug-in installation folder, and click **Next**.

5 On the Ready to Install the Plug-in page of the wizard, review the information and click **Install**.

6 After the installation completes, click **Finish**.

Deploy the vCenter Server Appliance with an Embedded Platform Services Controller

When you choose to deploy the vCenter Server Appliance with an embedded Platform Services Controller, you deploy the Platform Services Controller and vCenter Server as one appliance.

IMPORTANT Concurrent deployments of vCenter Server Appliances with embedded Platform Services Controllers are not supported. You must deploy the vCenter Server Appliance instances with embedded Platform Services Controllers in a sequence.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server Appliance installer.
- Install the Client Integration Plug-In.
- Verify that the ESXi host on which you deploy the vCenter Server Appliance is not in lockdown or maintenance mode.
- If you plan to use NTP servers for time synchronization, make sure that the time between the NTP servers and the ESXi host is synchronized.

Procedure

1 In the software installer directory, double-click **vcsa-setup.html**.

2 Wait up to three seconds for the browser to detect the Client Integration Plug-in and allow the plug-in to run on the browser when prompted.

3 On the Home page, click **Install** to start the vCenter Server Appliance deployment wizard.

4 Read and accept the license agreement, and click **Next**.

5 Connect to the target ESXi host on which you want to deploy the vCenter Server Appliance and click **Next**.

   a Enter the FQDN or the IP address of the ESXi host to connect to.

   b Enter the user name and the password of a user who has administrative privileges on the ESXi host, for example, the root user.

6 (Optional) Accept the certificate warning, if any, by clicking **Yes**.

7 On the Set up virtual machine page, enter the vCenter Server Appliance name, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

8 In the Select deployment type page, select **Install vCenter Server with an embedded Platform Services Controller** and click **Next**.

   This option deploys an appliance in which both the Platform Services Controller and vCenter Server are installed.

9 Create a new vCenter Single Sign-On domain or join an existing domain.

IMPORTANT Although you can select to join a vCenter Single Sign-On domain, you should consider the vCenter Server Appliance with an embedded Platform Services Controller as a standalone deployment and do not use it for replication of infrastructure data.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On server. a Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*your_domain_name*, where *your_domain_name* is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and to vCenter Server as adminstrator@*your_domain_name*. b Enter the domain name, for example **`vsphere.local`**. c Enter the site name for vCenter Single Sign-On. The site name is important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site. You cannot change the name after installation. The supported characters are alphanumeric characters and dash (-).
Join a Single Sign-On domain in an existing Platform Services Controller	Joins a new vCenter Single Sign-On server to a vCenter Single Sign-On domain in an existing Platform Services Controller. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. a Type the fully qualified domain name (FQDN) or IP address of the Platform Services Controller that contains the vCenter Single Sign-On server to join. b Type the password of the vCenter Single Sign-On administrator account. c Type the HTTPS port to use for communication with the Platform Services Controller and click **Next**. d Select whether to create or join an existing vCenter Single Sign-On site.

10 Click **Next**.

11 In the Select appliance size page of the wizard, select the vCenter Server Appliance size for your vSphere inventory, and click **Next**.

Option	Description
Tiny (up to 10 hosts, 100 VMs)	Deploys an appliance with 2 CPUs and 8 GB of memory.
Small (up to 100 hosts, 1,000 VMs)	Deploys an appliance with 4 CPUs and 16 GB of memory.
Medium (up to 400 hosts, 4,000 VMs)	Deploys an appliance with 8 CPUs and 24 GB of memory.
Large (up to 1,000 hosts, 10,000 VMs)	Deploys an appliance with 16 CPUs and 32 GB of memory.

12 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

13 Select the type of database that you want to use and click **Next**.

Option	Description
Use an embedded database (vPostgres)	Configures vCenter Server in the appliance to use the embedded PostgreSQL database. This database is suitable for small scale deployments.
Use an Oracle database	Configures vCenter Server in the appliance to use an existing external Oracle database. a Enter the IP address or the FQDN of the machine on which the Oracle database is installed. b Enter the port to use for communication with the Oracle database. c Enter the database instance name. d Enter the database user name and password. IMPORTANT Make sure that you provide correct credentials. Otherwise, the deployment might fail.

14 On the Network Settings page, set up the network settings.

The IP address or the FQDN of the appliance is used as a system name. It is recommended to use an FQDN. However, if you want to use an IP address, use static IP address allocation for the appliance, because IP addresses allocated by DHCP might change.

Option	Action
Choose a network	Select the network to connect to. The networks displayed in the drop-down menu depend on the ESXi network settings. Non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu.
IP Address family	Select the IP version of the appliance. You can select either IPv4 or IPv6.
Network type	Select how to allocate the IP address of the appliance. ■ **Static** You are prompted to enter the IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment.
FQDN (Optional)	Enter a preferred fully qualified domain name (FQDN) of the appliance.

If you use an IP address as a system name, you cannot change the IP address and update the DNS settings after deployment.

15 Configure the time settings in the appliance, optionally select **Enable SSH** to secure the connection, and click **Next**.

Option	Description
Synchronize appliance time with ESXi host	Enables periodic time synchronization, and VMware Tools sets the time of the guest operating system to be the same as the time of the ESXi host.
Use NTP servers (separated by commas)	Uses a Network Time Protocol server for synchronizing the time. If you select this option, you must enter the names of the NTP servers separated by commas.

16 In the Ready to complete page, review the deployment settings for the vCenter Server Appliance, and click **Finish** to complete the deployment process.

17 (Optional) After the deployment completes, click the **https://*vcenter_server_appliance_IP_address*/vsphere-client** link to start the vSphere Web Client and log in to the vCenter Server instance in the vCenter Server Appliance.

18 Click **Close** to exit the wizard.

Deploying a vCenter Server Appliance with an External Platform Services Controller

You can deploy a vCenter Server Appliance with an external Platform Services Controller. This way you deploy two different appliances.

To have the Platform Services Controller and the vCenter Server instance deployed as two different appliances, first deploy the Platform Services Controller, then deploy vCenter Server and the vCenter Server components as another virtual appliance, and register the vCenter Server Appliance to the Platform Services Controller.

IMPORTANT Concurrent deployments of vCenter Server Appliances and Platform Services Controller appliances are not supported. You must deploy the Platform Services Controller appliances and vCenter Server Appliances in a sequence.

IMPORTANT Before deploying a vCenter Server Appliance with an external Platform Services Controller, synchronize the clocks on the vSphere network. Time skew on the virtual machines might cause deployment failure. For instructions on synchronizing the clocks on your vSphere network, see "Synchronizing Clocks on the vSphere Network," on page 209.

Deploy a Platform Services Controller Appliance

If you plan to deploy the vCenter Server Appliance with an external Platform Services Controller, deploy a Platform Services Controller appliance first. The Platform Services Controller appliance contains all of the necessary services, such as vCenter Single Sign-On and License Service, which can be shared between multiple vCenter Server instances.

IMPORTANT You can deploy many Platform Services Controller appliances and join them to the same vCenter Single Sign-On domain. Concurrent deployments of Platform Services Controllers are not supported. You must deploy the Platform Services Controllers in a sequence.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server Appliance installer.
- Install the Client Integration Plug-In.
- Verify that the ESXi host on which you deploy the vCenter Server Appliance is not in lockdown or maintenance mode.
- If you plan to use NTP servers for time synchronization, make sure that the time between the NTP servers and the ESXi host is synchronized.

Procedure

1 In the software installer directory, double-click **vcsa-setup.html**.

2 Wait up to three seconds for the browser to detect the Client Integration Plug-in and allow the plug-in to run on the browser when prompted.

3 On the Home page, click **Install** to start the vCenter Server Appliance deployment wizard.

4 Read and accept the license agreement, and click **Next**.

5 Connect to the target ESXi host on which you want to deploy the vCenter Server Appliance and click **Next**.

   a Enter the FQDN or the IP address of the ESXi host to connect to.

   b Enter the user name and the password of a user who has administrative privileges on the ESXi host, for example, the root user.

6 On the Set up virtual machine page, enter the vCenter Server Appliance name, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

7 (Optional) Accept the certificate warning, if any, by clicking **Yes**.

8 In the Select a deployment type page, select **Install Platform Services Controller** and click **Next**.

9 Create a new vCenter Single Sign-On domain or join an existing domain.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On server. a Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*your_domain_name*, where *your_domain_name* is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and to vCenter Server as adminstrator@*your_domain_name*. b Enter the domain name, for example **`vsphere.local`**. c Enter the site name for vCenter Single Sign-On. The site name is important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site. You cannot change the name after installation. The supported characters are alphanumeric characters and dash (-).
Join a Single Sign-On domain in an existing Platform Services Controller	Joins a new vCenter Single Sign-On server to a vCenter Single Sign-On domain in an existing Platform Services Controller. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. a Type the fully qualified domain name (FQDN) or IP address of the Platform Services Controller that contains the vCenter Single Sign-On server to join. b Type the password of the vCenter Single Sign-On administrator account. c Type the HTTPS port to use for communication with the Platform Services Controller and click **Next**. d Select whether to create or join an existing vCenter Single Sign-On site.

   When you select to join an existing vCenter Single Sign-On domain, you enable the Enhanced Linked Mode feature. Your Platform Services Controller will replicate infrastructure data with the joined vCenter Single Sign-On server.

10 Click **Next**.

11 In the Select appliance size page of the wizard click **Next**.

   You deploy a Platform Services Controller appliance with 2 CPUs and 2 GB memory.

12 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

13 On the Network Settings page, set up the network settings.

The IP address or the FQDN of the appliance is used as a system name. It is recommended to use an FQDN. However, if you want to use an IP address, use static IP address allocation for the appliance, because IP addresses allocated by DHCP might change.

Option	Action
Choose a network	Select the network to connect to. The networks displayed in the drop-down menu depend on the ESXi network settings. Non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu.
IP Address family	Select the IP version of the appliance. You can select either IPv4 or IPv6.
Network type	Select how to allocate the IP address of the appliance. ■ **Static** You are prompted to enter the IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment.
FQDN (Optional)	Enter a preferred fully qualified domain name (FQDN) of the appliance.

If you use an IP address as a system name, you cannot change the IP address and update the DNS settings after deployment.

14 Configure the time settings in the appliance, optionally select **Enable SSH** to secure the connection, and click **Next**.

Option	Description
Synchronize appliance time with ESXi host	Enables periodic time synchronization, and VMware Tools sets the time of the guest operating system to be the same as the time of the ESXi host.
Use NTP servers (separated by commas)	Uses a Network Time Protocol server for synchronizing the time. If you select this option, you must enter the names of the NTP servers separated by commas.

15 In the Ready to complete page, review the deployment settings for the vCenter Server Appliance, and click **Finish** to complete the deployment process.

What to do next

You can now deploy the vCenter Server Appliance and connect it to the Platform Services Controller.

Deploy the vCenter Server Appliance

Deploy the vCenter Server Appliance after you deploy the Platform Services Controller appliance or install a Platform Services Controller on a Windows virtual machine or physical server.

IMPORTANT Concurrent deployments of vCenter Server Appliances are not supported. If you want to deploy many vCenter Server Appliances and register them with the same Platform Services Controller or Platform Services Controller appliance, deploy the vCenter Server Appliances one by one in a sequence.

Prerequisites

- Verify that your system meets the minimum software and hardware requirements.
- Download the vCenter Server Appliance installer.
- Install the Client Integration Plug-In.

- Verify that the ESXi host on which you deploy the vCenter Server Appliance is not in lockdown or maintenance mode.
- If you plan to use NTP servers for time synchronization, make sure that the time between the NTP servers and the ESXi host is synchronized.

Procedure

1. In the software installer directory, double-click **vcsa-setup.html**.
2. Wait up to three seconds for the browser to detect the Client Integration Plug-in and allow the plug-in to run on the browser when prompted.
3. On the Home page, click **Install** to start the vCenter Server Appliance deployment wizard.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the target ESXi host on which you want to deploy the vCenter Server Appliance and click **Next**.

   a. Enter the FQDN or the IP address of the ESXi host to connect to.

   b. Enter the user name and the password of a user who has administrative privileges on the ESXi host, for example, the root user.
6. (Optional) Accept the certificate warning, if any, by clicking **Yes**.
7. On the Set up virtual machine page, enter the vCenter Server Appliance name, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).
8. In the Select deployment type page, select **Install vCenter Server** and click **Next**.
9. Provide the system name of a Platform Services Controller that you already installed, enter the vCenter Single Sign-On password, and click **Next**.

   If you deployed a Platform Services Controller appliance, provide the IP address of the newly deployed appliance. If you installed a Platform Services Controller on Windows, provide the system name of the host machine on which you installed the Platform Services Controller.
10. In the Select appliance size page of the wizard, select the vCenter Server Appliance size depending on the vSphere inventory size, and click **Next**.

Option	Description
Tiny (up to 10 hosts, 100 VMs)	Deploys an appliance with 2 CPUs and 8 GB of memory.
Small (up to 100 hosts, 1,000 VMs)	Deploys an appliance with 4 CPUs and 16 GB of memory.
Medium (up to 400 hosts, 4,000 VMs)	Deploys an appliance with 8 CPUs and 24 GB of memory.
Large (up to 1,000 hosts, 10,000 VMs)	Deploys an appliance with 16 CPUs and 32 GB of memory.

11. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

12 Select the type of database that you want to use and click **Next**.

Option	Description
Use an embedded database (vPostgres)	Configures vCenter Server in the appliance to use the embedded PostgreSQL database. This database is suitable for small scale deployments.
Use an Oracle database	Configures vCenter Server in the appliance to use an existing external Oracle database. a Enter the IP address or the FQDN of the machine on which the Oracle database is installed. b Enter the port to use for communication with the Oracle database. c Enter the database instance name. d Enter the database user name and password. IMPORTANT Make sure that you provide correct credentials. Otherwise, the deployment might fail.

13 On the Network Settings page, set up the network settings.

The IP address or the FQDN of the appliance is used as a system name. It is recommended to use an FQDN. However, if you want to use an IP address, use static IP address allocation for the appliance, because IP addresses allocated by DHCP might change.

Option	Action
Choose a network	Select the network to connect to. The networks displayed in the drop-down menu depend on the ESXi network settings. Non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu.
IP Address family	Select the IP version of the appliance. You can select either IPv4 or IPv6.
Network type	Select how to allocate the IP address of the appliance. ■ **Static** You are prompted to enter the IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment.
FQDN (Optional)	Enter a preferred fully qualified domain name (FQDN) of the appliance.

If you use an IP address as a system name, you cannot change the IP address and update the DNS settings after deployment.

14 Configure the time settings in the appliance, optionally select **Enable SSH** to secure the connection, and click **Next**.

Option	Description
Synchronize appliance time with ESXi host	Enables periodic time synchronization, and VMware Tools sets the time of the guest operating system to be the same as the time of the ESXi host.
Use NTP servers (separated by commas)	Uses a Network Time Protocol server for synchronizing the time. If you select this option, you must enter the names of the NTP servers separated by commas.

15 In the Ready to complete page, review the deployment settings for the vCenter Server Appliance, and click **Finish** to complete the deployment process.

16 (Optional) After the deployment completes, click the **https://*vcenter_server_appliance_IP_address*/vsphere-client** link to start the vSphere Web Client and log in to the vCenter Server instance in the vCenter Server Appliance.

17 Click **Close** to exit the wizard.

Troubleshooting vCenter Server Installation or Deployment 10

The vCenter Server installation or deployment troubleshooting topics provide solutions to problems that you might encounter during the vCenter Server installation or vCenter Server Appliance deployment process.

This chapter includes the following topics:

Collecting Logs for Troubleshooting a vCenter Server Installation or Upgrade

You can collect installation or upgrade log files for vCenter Server. If an installation or upgrade fails, checking the log files can help you identify the source of the failure.

You can choose the Installation Wizard method or the manual method for saving and recovering log files for a vCenter Server for Windows installation failure.

You can also collect deployment log files for vCenter Server Appliance.

- Collect Installation Logs by Using the Installation Wizard on page 246

  You can use the Setup Interrupted page of the installation wizard to browse to the generated `.zip` file of the vCenter Server for Windows installation log files.

- Retrieve Installation Logs Manually on page 246

  You can retrieve the installation log files manually for examination.

- Collect Deployment Log Files for the vCenter Server Appliance on page 246

  If the vCenter Server Appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

- Export a vCenter Server Support Bundle for Troubleshooting on page 247

  If you want to export the support bundle of the vCenter Server instance in the vCenter Server Appliance for troubleshooting, you can do that by using the URL displayed on the DCUI home screen.

Collect Installation Logs by Using the Installation Wizard

You can use the Setup Interrupted page of the installation wizard to browse to the generated `.zip` file of the vCenter Server for Windows installation log files.

If the installation fails, the Setup Interrupted page appears with the log collection check boxes selected by default.

Procedure

1 Leave the check boxes selected and click **Finish**.

The installation files are collected in a `.zip` file on your desktop, for example, `VMware-VCS-logs-`*`time-of-installation-attempt`*`.zip`, where *time-of-installation-attempt* displays the year, month, date, hour, minutes, and seconds of the installation attempt.

2 Retrieve the log files from the `.zip` file on your desktop.

What to do next

Examine the log files to determine the cause of failure.

Retrieve Installation Logs Manually

You can retrieve the installation log files manually for examination.

Procedure

1 Navigate to the installation log file locations.

- `%PROGRAMDATA%\VMware\vCenterServer\logs` directory, usually `C:\ProgramData\VMware\vCenterServer\logs`
- `%TEMP%` directory, usually `C:\Users\`*`username`*`\AppData\Local\Temp`

The files in the `%TEMP%` directory include `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log`, and `vim-vcs-msi.log`.

2 Open the installation log files in a text editor for examination.

Collect Deployment Log Files for the vCenter Server Appliance

If the vCenter Server Appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

The full path to the log files is displayed in the vCenter Server Appliance deployment wizard.

In case of firstboot failure, you can download the support bundle on a Windows host machine and examine the log files to determine which firstboot script failed. See "Export a vCenter Server Support Bundle for Troubleshooting," on page 247.

Procedure

1 On the Windows machine that you use for deploying the vCenter Server Appliance, navigate to the log files folder.

If you are logged in as an administrator, by default this is the `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller` folder.

2 Open the installation log files in a text editor for examination.

Export a vCenter Server Support Bundle for Troubleshooting

If you want to export the support bundle of the vCenter Server instance in the vCenter Server Appliance for troubleshooting, you can do that by using the URL displayed on the DCUI home screen.

You can also collect the support bundle from the vCenter Server Appliance Bash shell, by running the `vc-support.sh` script.

The support bundle is exported in `.tgz` format.

Procedure

1 Log in to the Windows host machine on which you want to download the bundle.

2 Open a Web browser and enter the URL to the support bundle displayed in the DCUI.

https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3 Enter the user name and password of the root user.

4 Click **Enter**.

The support bundle is downloaded as `.tgz` file on your Windows machine.

5 (Optional) To determine which firstboot script failed, examine the `firstbootStatus.json` file.

If you ran the `vc-support.sh` script in the vCenter Server Appliance Bash shell, to examine the `firstbootStatus.json` file, run

```
cat /var/log/firstboot/firstbootStatus.json
```

Attempt to Install a Platform Services Controller After a Prior Installation Failure

When you want to replicate Platform Services Controller data, you might not be able to join a vCenter Single Sign-On domain in an existing Platform Services Controller.

Problem

When you try to install a Platform Services Controller, either embedded or external, and join the Platform Services Controller to a vCenter Single Sign-On domain or site, the installation might fail and the failure might leave incomplete data in the Platform Services Controller federation.

Cause

The Platform Services Controller data is not cleaned up when an installation of a Platform Services Controller fails. Consider the following scenario:

1 Install Platform Services Controller A.

2 When you try to install Platform Services Controller B and join it to the same domain as Platform Services Controller A, the installation fails.

3 Second attempt to install Platform Services Controller B and join it to the same domain as Platform Services Controller A fails, because Platform Services Controller A contains incomplete data.

Solution

1 Log in as an administrator to the machine on which you install Platform Services Controller A.

2 At the command prompt navigate to the `vdcleavefed` command.

The `vdcleavefed` command is located at `C:\Program Files\VMware\vCenter Server\vmdird\` on Windows and `/usr/lib/vmware-vmdir/bin/` on Linux.

3 Run the `vdcleavefed` command to delete the data.

```
vdcleavefed -h Platform-Services-Controller-B-System-Name -u Administrator
```

4 Install Platform Services Controller B.

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

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

Problem

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

Cause

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

Solution

◆ Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version. See the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

After You Install vCenter Server or Deploy the vCenter Server Appliance 11

After you install vCenter Server or deploy the vCenter Server Appliance, consider these postinstallation options before adding inventory for the vCenter Server to manage.

This chapter includes the following topics:

Log in to vCenter Server by Using the vSphere Web Client

Log in to vCenter Server by using the vSphere Web Client to manage your vSphere inventory.

Prerequisites

If you want to use vCenter Server 5.0 with vSphere Web Client, verify that the vCenter Server 5.0 system is registered with vSphere Web Client.

If you want to use vCenter Server 5.1 or vCenter Server 5.5 with vSphere Web Client, verify that vCenter Server is installed and that both vCenter Server and vSphere Web Client point to the same vCenter Single Sign-On instance.

In vSphere 6.0, the vSphere Web Client is installed as part of the vCenter Server on Windows or the vCenter Server Appliance deployment. This way, the vSphere Web Client always points to the same vCenter Single Sign-On instance.

Procedure

1. Open a Web browser and enter the URL for the vSphere Web Client: **`https://`*`client-hostname`*`/vsphere-client`**.
2. Enter the credentials of a user who has permissions on vCenter Server, and click **Login**.

3 If a warning message about an untrusted SSL certificate appears, select the appropriate action based on your security policy.

Option	Action
Ignore the security warning for this login session only.	Click **Ignore**.
Ignore the security warning for this login session, and install the default certificate so that the warning does not appear again.	Select **Install this certificate and do not display any security warnings for this server** and click **Ignore**. Select this option only if using the default certificate does not present a security problem in your environment.
Cancel and install a signed certificate before proceeding.	Click **Cancel** and ensure that a signed certificate is installed on the vCenter Server system before you attempt to connect again.

The vSphere Web Client connects to all the vCenter Server systems on which the specified user has permissions, allowing you to view and manage your inventory.

Collect vCenter Server Log Files

After you install vCenter Server, you can collect the vCenter Server log files for diagnosing and troubleshooting purposes.

Procedure

1 Log in as an administrator on the Windows machine where vCenter Server is installed.

2 Generate the log bundle.

- Navigate to **Start > Programs > VMware > Generate vCenter Server log bundle**.

  You can generate vCenter Server log bundles even if you are unable to connect to the vCenter Server by using the vSphere Web Client.

- In the command prompt, navigate to `*installation_directory*\VMware\vCenter Server\bin` and run the `vc-support.bat` command.

The log files for the vCenter Server system are generated and saved in a `.tgz` archive on your desktop.

Install or Upgrade vSphere Authentication Proxy

Install vSphere Authentication Proxy to enable ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy by removing the need to store Active Directory credentials in the host configuration.

If an earlier version of the vSphere Authentication Proxy is installed on your system, this procedure upgrades the vSphere Authentication Proxy to the current version.

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. vSphere Authentication Proxy is supported with vCenter Server versions 5.0 and later.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server instance 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 Web Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Install Microsoft .NET Framework 3.5 on the machine where you want to install vSphere Authentication Proxy.
- Verify that you have administrator privileges.
- Verify that the host machine has a supported processor and operating system.
- 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 vSphere 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`.
- Download the vCenter Server installer.

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Authentication Proxy, if you are not using the default location.
- The address and credentials for the vCenter Server that vSphere Authentication Proxy will connect to: IP address or name, HTTP port, user name, and password.
- The host name or IP address to identify vSphere Authentication Proxy on the network.

Procedure

1. Add the host machine where you will install the authentication proxy service to the domain.
2. Use the Domain Administrator account to log in to the host machine.
3. In the software installer directory, double-click the `autorun.exe` file to start the installer.
4. Select **VMware vSphere Authentication Proxy** and click **Install**.
5. Follow the wizard prompts to complete the installation or upgrade.

   During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

When you install the vSphere Authentication Proxy service, the installer creates a domain account with appropriate privileges to run the authentication proxy service. The account name begins with the prefix `CAM-` and has a 32-character, randomly generated password associated with it. The password is set to never expire. Do not change the account settings.

What to do next

Configure ESXi to use vSphere Authentication Proxy to join a domain. See the *vSphere Security* documentation.

Uninstall vCenter Server

You must have administrator privileges to uninstall VMware vCenter Server.

IMPORTANT If you are using the embedded PostgreSQL database, uninstalling vCenter Server causes the embedded database to be uninstalled, and all data is lost.

Prerequisites

If you are uninstalling the vCenter Server system, remove the hosts from the Hosts and Clusters inventory.

Procedure

1 As an administrator user on the Windows system, click **Start > Control Panel > Programs and Features**.

2 Select **VMware vCenter Server** from the list and click **Remove**.

3 Click **Remove** to confirm that you want to remove the program.

4 Click **Finish**.

Repointing the Connections Between vCenter Server and Platform Services Controller

Joining external Platform Services Controllers in the same vCenter Single Sign-On domain, ensures high availability of your system.

If your environment contains external Platform Services Controllers that replicate the infrastructure data within a single domain, you can redirect the vCenter Server instances and vCenter Server Appliances to another Platform Services Controller. As long as the Platform Services Controllers are in the same domain, if a Platform Services Controller stops responding, you can redirect the vCenter Server instances and vCenter Server Appliances to another Platform Services Controller within the domain.

Example: Repoint a vCenter Server Appliance to Another External Platform Services Controller

If you deploy the vCenter Server Appliance with an external Platform Services Controller and then deploy another Platform Services Controller appliance and join it to the vCenter Single Sign-On domain in the first Platform Services Controller, you can repoint the vCenter Server Appliance to the other Platform Services Controller in the domain at any time.

Consider the following scenario:

1 Deploy a Platform Services Controller appliance A.

2 Deploy a Platform Services Controller appliance B, and join it to the vCenter Single Sign-On domain in Platform Services Controller A.

3 Deploy a vCenter Server Appliance and register it with the Platform Services Controller appliance A.

4 If Platform Services Controller appliance A stops responding, repoint the vCenter Server Appliance to Platform Services Controller appliance B.

   a Log in to the vCenter Server Appliance Linux console as root.

   b Repoint the vCenter Server Appliance to Platform Services Controller appliance B.

   ```
   /usr/lib/vmware-vmafd/bin/vmafd-cli set-dc-name --server-name localhost --dc-name system-name-of-platform-services-controller-B
   ```

   Here, *system-name-of-platform-services-controller-B* is the system name used to identify the Platform Services Controller B. This system name must be an FQDN or a static IP address.

   c (Optional) If Platform Services Controller B runs on an HTTPS port that is different from the HTTPS port of Platform Services Controller A, you must also update the port number.

   ```
   /usr/lib/vmware-vmafd/bin/vmafd-cli set-dc-port --server-name localhost --dc-port https-port-of-platform-services-controller-B
   ```

   d Use the `service-control` CLI to stop the services in the vCenter Server Appliance.

   ```
   service-control --stop --all
   ```

   e Use the `service-control` CLI to start the services in the vCenter Server Appliance.

   ```
   service-control --start --all
   ```

f Log in to the vCenter Server instance in the vCenter Server Appliance by using the vSphere Web Client to verify that the vCenter Server is up and running and can be managed.

Example: Repoint vCenter Server to Another External Platform Services Controller

If you install vCenter Server with an external Platform Services Controller and then install another Platform Services Controller and join it to the vCenter Single Sign-On domain in the first Platform Services Controller, you can repoint the vCenter Server to the other at any time.

Consider the following scenario:

1 Install a Platform Services Controller A.

2 Install a Platform Services Controller B, and join it to the vCenter Single Sign-On domain in Platform Services Controller A.

3 Install vCenter Server and register it with the Platform Services Controller A.

4 If Platform Services Controller A stops responding, repoint the vCenter Server instance to Platform Services Controller B.

a Log in as an administrator to the virtual machine or physical server on which you installed vCenter Server.

b Open the command prompt.

c Repoint the vCenter Server instance to Platform Services Controller B.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli set-dc-name --server-name
localhost --dc-name system-name-of-platform-services-controller-B
```

Here, *system-name-of-platform-services-controller-B* is the system name used to identify the Platform Services Controller B. This system name must be an FQDN or a static IP address.

d (Optional) If Platform Services Controller B runs on an HTTPS port that is different from the HTTPS port of Platform Services Controller A, you must also update the port number.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli set-dc-port --server-name
localhost --dc-port https-port-of-platform-services-controller-B
```

e Use the `service-control` CLI to stop the vCenter Server services.

```
service-control --stop --all
```

f Use the `service-control` CLI to start the vCenter Server services.

```
service-control --start --all
```

g Log in to the vCenter Server instance by using the vSphere Web Client to verify that the vCenter Server is up and running and can be managed.

Backing Up and Restoring vCenter Server 12

You can use vSphere Data Protection to back up and restore a virtual machine (VM) that contains vCenter Server, a vCenter Server Appliance, or a Platform Services Controller.

IMPORTANT This documentation provides information about backing up and restoring vCenter Server with an embedded Platform Services Controller and vCenter Server Appliance with an embedded Platform Services Controller. For information on how to back up and restore vCenter Server with an external Platform Services Controller and vCenter Server Appliance with an external Platform Services Controller, see How to backup and restore vCenter Server 6.0 external deployment model.

vSphere Data Protection is a disk-based backup and recovery solution that is powered by EMC. vSphere Data Protection is fully integrated with vCenter Server and lets you manage backup jobs while storing backups in deduplicated destination storage locations. After you deploy and configure vSphere Data Protection, you can access vSphere Data Protection by using the vSphere Web Client interface to select, schedule, configure, and manage backups and recoveries of VMs. During a backup, vSphere Data Protection creates a quiesced snapshot of the VM. Deduplication is automatically performed with every backup operation.

In vSphere 6.0, to back up and restore a VM that contains vCenter Server, a vCenter Server Appliance, or a Platform Services Controller, you must do a full image backup, and the VM must meet the following requirements:

- The VM must have VMware Tools installed and running.
- The VM must use a fully qualified domain name (FQDN) with correct DNS resolution, or must be configured with a static IP address.

The following backups and recoveries are not supported:

- Incremental backups
- Differential backups
- Individual disk backups
- Virtual machines that have snapshots

You can also use vSphere Data Protection to restore a VM that contains vCenter Server instance directly on the ESXi host that is running the vSphere Data Protection Appliance when the vCenter Server service becomes unavailable or when you cannot access the vSphere Data Protection user interface by using the vSphere Web Client.

1 Deploy the vSphere Data Protection OVF Template on page 256

   Deploy vSphere Data Protection to back up and restore a VM that contains vCenter Server or the vCenter Server Appliance.

2 Configure vSphere Data Protection on page 257

During the initial vSphere Data Protection configuration you can configure the network settings and time zone information for your vSphere Data Protection Appliance. You use the vSphere Data Protection configuration wizard to register the vSphere Data Protection Appliance with vCenter Server.

3 Create a Backup Job in vSphere Data Protection on page 258

You can create backup jobs to associate the backup of a set of one or more VMs that contain vCenter Server or the vCenter Server Appliance with a backup schedule and specific retention policies.

4 Start Manually a Backup Job on page 259

A backup operation starts automatically according to the scheduled date, time, and frequency configured in the backup job. If you want to run an existing backup job immediately, you can start the process manually.

5 Restoring vCenter Server on page 260

After you back up a VM that contains vCenter Server or the vCenter Server Appliance, you can restore the backups to the original location or a new location.

Deploy the vSphere Data Protection OVF Template

Deploy vSphere Data Protection to back up and restore a VM that contains vCenter Server or the vCenter Server Appliance.

Prerequisites

- Verify that your ESXi version is 5.0 or later.
- If a firewall is enabled in your environment, verify that port 902 is open for communication between the vSphere Data Protection Appliance and the ESXi host. See the *vSphere Data Protection* documentation.
- Verify that the VMware Client Integration Plug-in is installed for your browser. For more information, see "Install the Client Integration Plug-In," on page 234.
- Use the vSphere Web Client to log in as an administrator to the vCenter Server instance that manages your environment.

Procedure

1 Select **vCenter > Datacenters**.

2 On the **Objects** tab, click **Actions** and select **Deploy OVF Template**.

3 Navigate to the location of the vSphere Data Protection Appliance `.ova` file and click **Open**.

4 Verify the OVF template details and click **Next**.

5 Review the template details, click **Next**, and follow the prompts of the wizard to accept the license agreement.

6 On the Select name and folder page, enter an FQDN for the vSphere Data Protection Appliance, select the folder or data center where you want to deploy the vSphere Data Protection Appliance, and click **Next**.

The vSphere Data Protection configuration uses the name that you enter to find the vSphere Data Protection Appliance in the vCenter Server inventory. Do not change the vSphere Data Protection Appliance name after installation.

7 Select the host on which to deploy the vSphere Data Protection Appliance and click **Next**.

8 Select the virtual disk format and the storage location for the vSphere Data Protection Appliance and click **Next**.

9. Select the destination network for the vSphere Data Protection Appliance and click **Next**.
10. On the Customize template page, enter the network settings such as the default gateway, DNS, network IP address, and netmask and click **Next**.

    Confirm that the IP addresses are correct and match the entry in the DNS server. If you enter incorrect IP addresses, you must redeploy the vSphere Data Protection Appliance.

    NOTE The vSphere Data Protection Appliance does not support DHCP. A static IP address is required.

11. On the Ready to complete page, confirm that all of the deployment options are correct, select **Power on after deployment**, and click **Finish**.

The vSphere Data Protection Appliance deployment process starts and the vSphere Data Protection Appliance boots in install mode.

What to do next

Configure the initial settings of vSphere Data Protection. See "Configure vSphere Data Protection," on page 257.

Configure vSphere Data Protection

During the initial vSphere Data Protection configuration you can configure the network settings and time zone information for your vSphere Data Protection Appliance. You use the vSphere Data Protection configuration wizard to register the vSphere Data Protection Appliance with vCenter Server.

Prerequisites

- Deploy the vSphere Data Protection Appliance.
- Read the *vSphere Data Protection Administration Guide* for the complete list of steps to configure vSphere Data Protection.
- Verify that enough disk space is available on the datastore. When an optional performance analysis test is run during the initial configuration of the appliance, 41 GB is required for each disk on each datastore. If the available space is not enough, the test reports a value of 0 for all of the read, write, and seek tests, and displays a final status of insufficient space.
- Use the vSphere Web Client to log in as an administrator to the vCenter Server instance that manages your environment.

Procedure

1. In the vSphere Web Client, select **vCenter Inventory Lists > Virtual Machines**.
2. Right-click the vSphere Data Protection Appliance and select **Open Console**.

   After the installation files load, the Welcome screen for the vSphere Data Protection menu appears.

3. In a Web browser, navigate to vSphere Data Protection Configuration Utility URL.

   https://*IP_address_VDP_Appliance*:8543/vdp-configure/

4. Log in as root.

   The default password is changeme.

   The vSphere Data Protection configuration wizard appears.

5. On the Network settings page of the wizard, enter or confirm the network and server information for the vSphere Data Protection Appliance, and click **Next**.

   Ensure that the values are populated correctly, otherwise the initial configuration fails.

6 Select the appropriate time zone for your vSphere Data Protection Appliance and click **Next**.

7 On the VDP credentials page, select a new root password for the virtual appliance and click **Next**.

8 On the vCenter Registration page, register the appliance with vCenter Server:

   a In the **vCenter username** text box, enter a vCenter Server user name.

   If the user belongs to a domain account, enter the user name by using the *DOMAIN\UserName* format.

   IMPORTANT If you enter the vCenter Single Sign-On administrator user name in the user principal name (UPN) format, the tasks related to vSphere Data Protection operations do not appear in the Recent Tasks pane of the vSphere Web Client. If you want to use the vCenter Single Sign-On administrator user name, enter the vCenter Single Sign-On user name in UPN format.

   b In the **vCenter password** text box, enter the vCenter Server password.

   c Enter a vCenter FQDN or IP address.

   d Change the default vCenter Server HTTP port.

   Enter a custom value for the HTTP port if you must connect to vCenter Server over the HTTP port, instead of the HTTPS port, which is used for all other communication.

   e Enter a vCenter HTTPS port (the default is 443).

   f Select the **Use vCenter for SSO authentication** check box.

   g (Optional) Click **Test Connection**.

   A connection success message appears. If this message does not appear, troubleshoot your settings and repeat this step until a successful message appears.

9 Click **Next** and respond to the wizard prompts to complete the configuration.

What to do next

Create a backup job with specific retention policy and backup schedule. For more information, see "Create a Backup Job in vSphere Data Protection," on page 258.

Create a Backup Job in vSphere Data Protection

You can create backup jobs to associate the backup of a set of one or more VMs that contain vCenter Server or the vCenter Server Appliance with a backup schedule and specific retention policies.

IMPORTANT This documentation provides information about backing up and restoring vCenter Server with an embedded Platform Services Controller and vCenter Server Appliance with an embedded Platform Services Controller. For information on how to back up and restore vCenter Server with an external Platform Services Controller and vCenter Server Appliance with an external Platform Services Controller, see How to backup and restore vCenter Server 6.0 external deployment model.

Prerequisites

- Deploy and configure the vSphere Data Protection Appliance.
- Use the vSphere Web Client to log in to the vCenter Server instance that manages your environment. Log in as the user with administrator privileges that was used during the vSphere Data Protection configuration.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Data Protection**.

2 From the **Backup Job Actions** menu, select **New** to run the Create new backup job wizard.

3 On the Job Type page, select **Guest Images** and click **Next**.

4 On the Data Type page, select **Full Image** and click **Next**.

You can see all the objects and virtual machines in the vCenter Server inventory.

5 On the Backup Targets page, select the VM that contains the vCenter Server instance you want to back up, and click **Next**.

6 On the Schedule page, select the schedule for the backup job and click **Next**.

7 On the Retention Policy page, select a retention period and click **Next**.

NOTE When you enter a new maintenance period that follows the expiration of a backup, the vSphere Data Protection Appliance removes its reference to the backup data and you cannot restore the expired backup. The vSphere Data Protection Appliance determines whether the backup data is used by any other restore point, and if the system determines that the data is not used, the data is removed and the disk capacity becomes available.

8 On the Name page, enter a name for the backup job and click **Next**.

9 On the Ready to Complete page, review the summary information for the backup job and click **Finish**.

The newly created backup job is listed on the **Backup** tab. The backup job starts automatically according to the configured schedule.

What to do next

- Run an existing backup job immediately . For more information, see "Create a Backup Job in vSphere Data Protection," on page 258.
- Restore a backed up vCenter Server or a vCenter Server Appliance. For more information, see "Restoring vCenter Server," on page 260.

Start Manually a Backup Job

A backup operation starts automatically according to the scheduled date, time, and frequency configured in the backup job. If you want to run an existing backup job immediately, you can start the process manually.

Prerequisites

- Deploy and configure the vSphere Data Protection Appliance.
- Create a backup job. See "Create a Backup Job in vSphere Data Protection," on page 258.
- Use the vSphere Web Client to log in to the vCenter Server instance that manages your environment. Log in as the user with administrator privileges that was used during the vSphere Data Protection configuration.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Data Protection**.

2 On the **Backup** tab, select the backup job that you want to run.

3 Click **Backup now**, and select **Backup all sources**.

A dialog box confirms that the backup operation was successfully initiated.

What to do next

Restore a backed up vCenter Server or vCenter Server Appliance. For more information, see "Restoring vCenter Server," on page 260.

Restoring vCenter Server

After you back up a VM that contains vCenter Server or the vCenter Server Appliance, you can restore the backups to the original location or a new location.

You can restore VMs to the original location by either overwriting the backed up VM or by creating a new VM that contains the restored vCenter Server or vCenter Server Appliance on the same ESXi host. You can also restore the VM on a new ESXi host.

You can restore a VM on the ESXi host that is running the vSphere Data Protection Appliance. The direct-to-host emergency restore operation lets you restore a VM that contains vCenter Server instance when vCenter Server becomes unavailable or when the user cannot access the vSphere Data Protection user interface by using the vSphere Web Client.

Restore vCenter Server to the Original Location

You can restore full image backups of VMs that contain vCenter Server or the vCenter Server Appliance manually by using the Restore backup wizard.

IMPORTANT This documentation provides information about backing up and restoring vCenter Server with an embedded Platform Services Controller and vCenter Server Appliance with an embedded Platform Services Controller. For information on how to back up and restore vCenter Server with an external Platform Services Controller and vCenter Server Appliance with an external Platform Services Controller, see How to backup and restore vCenter Server 6.0 external deployment model.

Prerequisites

- Deploy and configure the vSphere Data Protection Appliance.
- Back up a VM with running vCenter Server or the vCenter Server Appliance. See, "Create a Backup Job in vSphere Data Protection," on page 258.
- Use the vSphere Web Client to log in to the vCenter Server instance that manages your environment. Log in as the user with administrator privileges that was used during the vSphere Data Protection configuration.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Data Protection**.

2 Click the **Restore** tab.

3 (Optional) Filter the backups to narrow your search.

4 Select a VM listed in the Name column, and select one or more backup items that you want to restore.

When you select a VM, you can see the list the performed backups for that VM.

5 Click **Restore** to start the Restore backup wizard.

6 On the Select Backup page, verify that the list of backups is correct, remove the backups that you want to exclude from the restore operation, and click **Next**.

7 On the Set Restore Options page, leave the **Restore to Original Location** check box selected.

IMPORTANT If the virtual disk of the original VM has been removed or deleted, you cannot restore the VM to its original location. The VMDK must be restored to a new location.

8 (Optional) Under **Advanced options**, select a new datastore to power on the VM after it is restored and to reconnect the NIC.

9 Click **Next**.

10 On the Ready to complete page, review the summary of your restore requests, and click **Finish** to start the restore operation.

NOTE If in Step 8 you selected to reconnect NIC during the restore process, verify that the network configuration for the newly created VM is correct. The new VM NIC might use the same IP address as the original VM, which causes conflicts.

An information dialog box confirms that the restore operation was successfully initiated. You can monitor the restore progress in the Recent Tasks pane.

Restore vCenter Server to a New Location

You can restore full image backups manually by using the Restore backup wizard.

IMPORTANT This documentation provides information about backing up and restoring vCenter Server with an embedded Platform Services Controller and vCenter Server Appliance with an embedded Platform Services Controller. For information on how to back up and restore vCenter Server with an external Platform Services Controller and vCenter Server Appliance with an external Platform Services Controller, see How to backup and restore vCenter Server 6.0 external deployment model.

Prerequisites

- Deploy and configure the vSphere Data Protection Appliance.
- Back up a VM with running vCenter Server or the vCenter Server Appliance. See, "Create a Backup Job in vSphere Data Protection," on page 258.
- Use the vSphere Web Client to log in to the vCenter Server instance that manages your environment. Log in as the user with administrator privileges that was used during the vSphere Data Protection configuration.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Data Protection**.

2 Click the **Restore** tab.

3 (Optional) Filter the backups to narrow your search.

4 Select a VM listed in the Name column, and select one or more backup items that you want to restore.

When you select a VM, you can see the list the performed backups for that VM.

5 Click **Restore** to start the Restore backup wizard.

6 On the Select Backup page, verify that the list of backups is correct, remove the backups that you want to exclude from the restore operation, and click **Next**.

7 On the Set Restore Options page, deselect the **Restore to Original Location** check box to set the restore options for each backup that you are restoring to a new location.

8 Enter the new VM name and click **Choose** to select a new host for the restored VM.

9 Select the datastore in which to restore the VM that contains vCenter Server or the vCenter Server Appliance, and click **Next**.

10 (Optional) Under **Advanced options**, select a new datastore to power on the VM after it is restored and to reconnect the NIC.

11 Click **Next**.

12 On the Ready to complete page, review the summary of your restore requests, and click **Finish** to start the restore operation.

Note If in Step 10 you selected to reconnect NIC during the restore process, confirm the network configuration for the newly created VM. The new VM NIC might use the same IP address as the original VM, which causes conflicts.

An information dialog box confirms that the restore operation was successfully initiated. You can monitor the restore progress in the Recent Tasks pane.

Restore vCenter Server with the Direct-to-Host Emergency Restore Operation

The direct-to-host emergency restore operation lets you restore the VM that contains vCenter Server or the vCenter Server Appliance when vCenter Server becomes unavailable or when you cannot access the vSphere Data Protection user interface by using the vSphere Web Client.

vSphere Data Protection depends on vCenter Server for many of the vSphere Data Protection core operations. When vCenter Server becomes unavailable, an emergency restore operation can restore the VM that contains the vCenter Server directly on the ESXi host that is running the vSphere Data Protection Appliance. The **Emergency Restore** tab displays a list of VMs that have been backed up by the vSphere Data Protection Appliance. These VMs containing vCenter Server instances can be restored as new VMs on the ESXi host where the vSphere Data Protection Appliance is running. For best practices, recommendations, and limitations of the emergency restore operation, see the *vSphere Data Protection* documentation.

Procedure

1 Log in as an administrator to the vSphere Client, click the **Summary** tab.

   a Under Host Management, select **Disassociate Host from vCenter Server**.

   b Click **Yes** when prompted to disassociate the host from vCenter Server.

2 In a Web browser, navigate to the vSphere Data Protection Configure Utility.

   https://*IP_address_VDP_Appliance*:8543/vdp-configure/.

3 On the **Emergency Restore** tab, select the VM that will serve as the restore point, and click **Restore**.

4 In the Host Credentials dialog box, enter valid host credentials and click **OK**.

5 In the Restore a Backup dialog box, enter a new name.

6 Select a datastore as the destination target for the backup, and click **Restore**.

⚠ **Caution** The datastore capacity size is listed. Make sure you select a datastore with enough disk space to accommodate the restore. Insufficient space causes the restore to fail.

7 In the Recent Tasks pane, check the progress to verify that the restore is submitted successfully.

Note The restored VM is listed in the inventory at the vSphere host level. Restoring to a more specific inventory path is not supported.

Index