# vSphere Upgrade

Update 2
Modified on 11 AUG 2020
VMware vSphere 6.0
VMware ESXi 6.0
vCenter Server 6.0

vmware®

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

https://docs.vmware.com/

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

# Contents

# About vSphere Upgrade

*vSphere Upgrade* describes how to upgrade VMware vSphere™ to the current version.

To move to the current version of vSphere by performing a fresh installation that does not preserve existing configurations, see the *vSphere Installation and Setup* documentation.

## Intended Audience

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

# Updated Information

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

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

| Revision | Description |
|---|---|
| 2 APR 2021 | VMware has rebranded the My VMware portal as VMware Customer Connect. We updated the *vSphere Upgrade* documentation to reflect this name change. |
| 11 AUG 2020 | At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we are replacing some of the terminology in our content. We have updated this guide to remove instances of non-inclusive language. |
| EN-001989-08 | Added port 5480 in Required Ports for vCenter Server and Platform Services Controller. |
| EN-001989-07 | Removed UDP from port 22 in Required Ports for vCenter Server and Platform Services Controller. |
| EN-001989-06 | ■ Updated information about port 514 in Required Ports for vCenter Server and Platform Services Controller.<br>■ Updated topic Using vSphere Update Manager to Perform Orchestrated Host Upgrades to remove unneeded /boot partition space requirement. |
| EN-001989-05 | ■ Updated About the boot.cfg File to add a reference to an example.<br>■ Updated TCP and UDP Ports for the vSphere Client to remove port 903.<br>■ Updated Repoint vCenter Server to Another External Platform Services Controller to improve the information in the task context and prerequisites. |
| EN-001989-04 | ■ Updated vCenter Server for Windows Hardware Requirements and vCenter Server Appliance Hardware Requirements to state that the hardware requirements for vCenter Server with an embedded Platform Services Controller and vCenter Server with an external Platform Services Controller are the same.<br>■ Updated Reconfigure Each vCenter Server Instance and Repoint It from an Embedded to External Platform Services Controller Instance to add a step for creating direct replication agreement between the embedded and the external Platform Services Controller instances if not present. |
| EN-001989-03 | ■ Updated information on port 22 in Required Ports for vCenter Server and Platform Services Controller.<br>■ Topics Upgrade the vCenter Server Appliance with Embedded vCenter Single Sign-On and Upgrade the vCenter Server Appliance with External vCenter Single Sign-On now contain prerequisites for the ports that must be open during the upgrade of the appliance.<br>■ Updated Install the Client Integration Plug-In to improve the information about the location of the executable file.<br>■ Revised the prerequisites and steps in Format a USB Flash Drive to Boot the ESXi Installation or Upgrade. |
| EN-001989-02 | ■ Updated information on ports 389, 636, 11711, and 11712 in Required Ports for vCenter Server and Platform Services Controller.<br>■ Minor revisions of the examples in Create an Installer ISO Image with a Custom Installation or Upgrade Script and Boot Options . |

| Revision | Description |
| --- | --- |
| EN-001989-01 | ■ Updated information on the number of vCenter Server instances in How vCenter Single Sign-On Affects Upgrades.<br>■ Updated the topic Reconfigure a Standalone vCenter Server with an Embedded Platform Services Controller to a vCenter Server with an External Platform Services Controller and added the topic Reconfigure Multiple Joined Instances of vCenter Server with an Embedded Platform Services Controller to vCenter Server with an External Platform Services Controller to improve the information about reconfiguring a standalone and multiple instances of vCenter Server with an embedded Platform Services Controller.<br>■ Updated the topic Configuring VMware vCenter Server - tc Server Settings in vCenter Server to remove the APJ port 8009 which is no longer required. |
| EN-001989-00 | Initial release. |

# Introduction to vSphere Upgrade 1

vSphere 6.0 has many options for upgrading your vSphere deployment. For a successful vSphere upgrade, you must understand the upgrade options, configuration details that impact the upgrade process, and 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. You use the vCenter Server system to pool and manage the resources of multiple hosts.

You can upgrade the vCenter Server system on a Windows virtual machine or physical server, or upgrade vCenter Server Appliance. vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running the vCenter Server system and the vCenter Server components.

Starting with vSphere 6.0, all prerequisite services for running vCenter Server and the vCenter Server components are bundled in the Platform Services Controller. Depending on the details of your existing vCenter Server configuration, you can upgrade to the vCenter Server system with an embedded or external Platform Services Controller. For details about vCenter Server 6.0 upgrade options, see About the vCenter Server 6.0 for Windows Upgrade Process and About the vCenter Server Appliance Upgrade Process.

For information on ESXi upgrade support, see Upgrade Options for ESXi 6.0.

When you upgrade to vSphere 6.0, you must perform all procedures in sequence to avoid possible data loss and to minimize downtime. You can perform the upgrade process for each component in only one direction. For example, after you upgrade to vCenter Server 6.0, you cannot revert to vCenter Server 5.x. With backups and some planning, however, you can restore your original software records. For information on the overall vSphere upgrade sequence, see vSphere Upgrade Process.

This chapter includes the following topics:

- How vCenter Single Sign-On Affects Upgrades
- vSphere Security Certificates Overview
- Enhanced Linked Mode Overview
- vCenter Server Example Upgrade Paths

# 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 upgrade to vCenter Server with an embedded Platform Services Controller, or to 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 upgrade to 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.

## How vSphere 6.0 Differs from vSphere 5.x

Some changes from vSphere 5.x to vSphere 6.0 impact the vCenter Server upgrade process. For a complete list of new features in vSphere 6.0, see the Release Notes for version 6.0 releases.

### VMware Platform Services Controller Introduced

The VMware Platform Services Controller contains common infrastructure services such as vCenter Single Sign-On, VMware certificate authority, licensing, and server reservation and registration services.

You can deploy a Platform Services Controller instance on the same virtual machine (VM) or physical server as vCenter Server, which is vCenter Server with an embedded Platform Services Controller instance. You can also deploy a Platform Services Controller instance on a separate machine or physical server, which is vCenter Server with an external Platform Services Controller instance. See vCenter Server Deployment Models.

### Enhanced Linked Mode

Starting with vSphere 6.0, the implementation of Linked Mode has changed. You no longer need to join vCenter Server instances to Linked Mode groups. You can access the replication functionality provided by Linked Mode in vSphere 5.5 by registering multiple vCenter Server instances to the same Platform Services Controller or joining Platform Services Controller instances in the same vCenter Single Sign-On domain.

To enable high availability between the vCenter Server instances in a single vCenter Single Sign-On domain, the vCenter Server instances must use the same site name.

Unlike the original Linked Mode, Enhanced Linked Mode is available and supported on vCenter Server on Windows and vCenter Server Appliance.

### vCenter Server Component Services Deployment

Starting with vSphere 6.0, vCenter Server component services are deployed in either the vCenter Server or Platform Services Controller group of services. vSphere common services can no longer be upgraded individually with vCenter Server 6.0.

The vCenter Server upgrade software migrates, upgrades, and configures existing vCenter Server 5.1 or vCenter Server 5.5 services as needed, migrating individually deployed vCenter Server 5.0 or vCenter Server 5.1 services to the appropriate service group during the upgrade process.

- vCenter Single Sign-On credentials, certificates, and ports are now part of the Platform Services Controller instance.
- Tagging data and licensing is part of the Platform Services Controller instance.
- Other services are part of the vCenter Server instance. For details, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0.
- You can now choose the destination folder for the upgrade software to use.

For more details about service deployment, see About the vCenter Server 6.0 for Windows Upgrade Process.

### Simple Upgrade Process Replaced

Upgrading to vCenter Server 6.0 with an embedded Platform Services Controller instance replaces the vCenter Server 5.1 or vCenter Server 5.5 simple upgrade process. The upgrade process migrates your vCenter Server 5.1 or vCenter Server 5.5 services to a vCenter Server 6.0 deployment with an embedded Platform Services Controller instance.

### Custom Upgrade Process Replaced

Upgrading to vCenter Server 6.0 with an external Platform Services Controller instance replaces the vCenter Server 5.1 or 5.5 Custom or separate upgrade process. When you upgrade your custom or distributed vCenter Server 5.1 or 5.5 instance, the upgrade process includes any vCenter Server 5.1 or 5.5 services that are deployed separately from vCenter Server. You do not need to upgrade them separately.

During the process of upgrading to vCenter Server 6.0 with an external Platform Services Controller deployment, any vCenter Server 5.1 or 5.5 services that are deployed on a separate VM or physical server from the vCenter Server are migrated to the same VM or physical server as the vCenter Server instance. vCenter Server components can no longer be deployed individually. For more details on service migration during upgrade, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0

### No Change of Deployment Model for Platform Services Controller During Upgrade

During the upgrade to vCenter Server 6.0 , you cannot change your deployment model. For example, if you deploy vCenter Server with an embedded Platform Services Controller instance, you cannot switch to vCenter Server with an external Platform Services Controller instance. You can only remove the Platform Services Controller instance.

After the upgrade, you can update your vCenter Server deployment by repointing the connections between vCenter Server and Platform Services Controller. You can also convert an embedded Platform Services Controller deployment to an external Platform Services Controller deployment.

### Database Changes

The vCenter Server 5.x embedded Microsoft SQL Server Express database is replaced with an embedded PostgreSQL database during the upgrade to vCenter Server 6.0. The maximum inventory size that applied for Microsoft SQL Server Express still applies for PostgreSQL.

### VMware vSphere Syslog Collector

For vCenter Server 6.0 for Windows, vSphere Syslog Collector is included in the vCenter Server group of services and continues to function exactly as for vCenter Server 5.5. However, it is no longer used for vCenter Server Appliance 6.0.

### VMware Syslog Service

For vCenter Server Appliance 6.0, vSphere Syslog Service is a support tool for logging that is included in the vCenter Server group of services. See vCenter Server Components and Services

## 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.

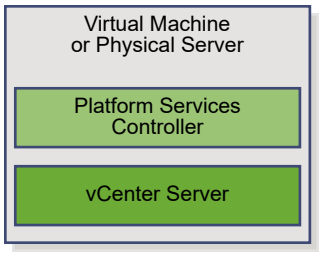
You first must deploy the Platform Services Controller on one virtual machine or physical server and then deploy vCenter Server on another virtual machine or physical server.

**Note** After you deploy vCenter Server with an embedded Platform Services Controller, you can reconfigure your topology and switch to vCenter Server with an external Platform Services Controller. This is a one-way process after which you cannot switch back to vCenter Server with an embedded Platform Services Controller. You can repoint the vCenter Server instance only to an external Platform Services Controller that is configured to replicate the infrastructure data within the same domain.

## 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.

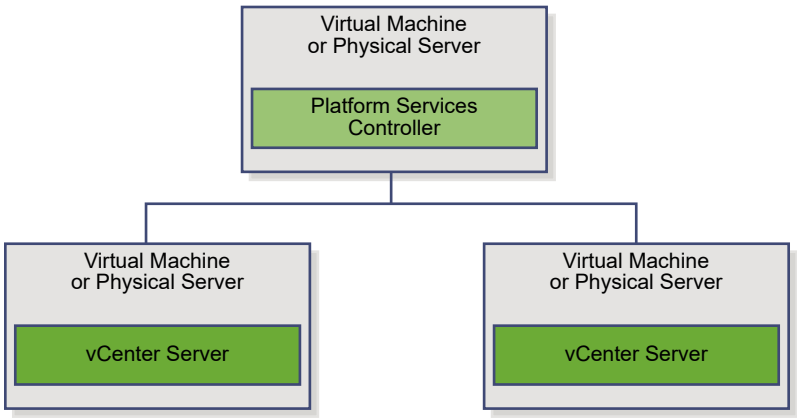
Installing with an embedded Platform Services Controller has the following disadvantages:

- 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

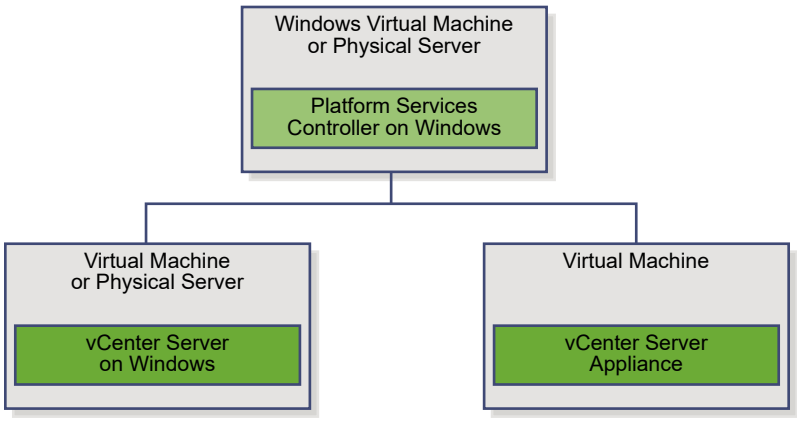
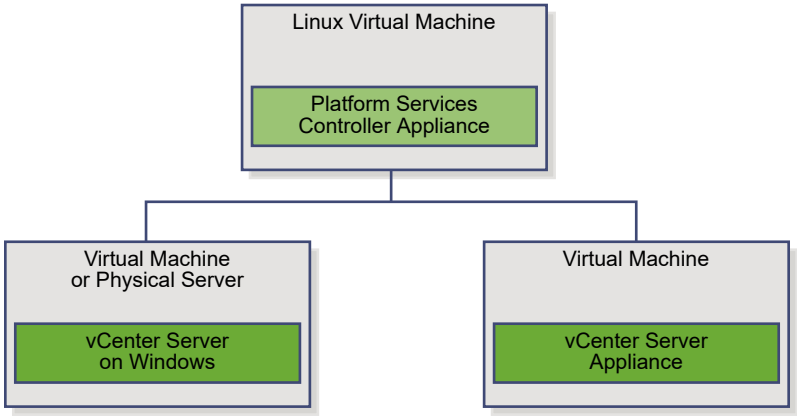



Figure 1-4. Example of a Mixed Operating Systems Environment with an External Platform Services Controller Appliance




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 Repoint vCenter Server to Another External Platform Services Controller.

# vSphere Upgrade Process

vSphere is a sophisticated product with multiple components to upgrade. For a successful vSphere upgrade, you must understand the sequence of tasks required.

Upgrading 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 Upgrade Requirements.

3 Verify that you have backed up your configuration.

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

5 Upgrade vCenter Server.

You can connect vCenter Server instances with external Platform Services Controller instances in an Enhanced Linked Mode configuration.

**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.

Concurrent upgrades are not supported and upgrade order matters. If you have multiple vCenter Server instances or services that are not installed on the same physical server or virtual machine (VM) as the vCenter Server instance, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0 and Mixed-Version Transitional Environments During vCenter Server Upgrades

Upgrade vCenter Server on a Windows VM or physical server or upgrade the vCenter Server Appliance. For the vCenter Server for Windows upgrade workflow, see About the vCenter Server 6.0 for Windows Upgrade Process. For the vCenter Server Appliance workflow, see About the vCenter Server Appliance Upgrade Process.

a Verify that your system meets the hardware and software requirements for upgrading vCenter Server. See vCenter Server for Windows Requirements or vCenter Server Appliance Requirements.

b Prepare your environment for the upgrade. See Chapter 3 Before Upgrading vCenter Server

c Create a worksheet with the information that you need for the upgrade. See Required Information for Upgrading vCenter Server for Windows or Required Information for Upgrading the vCenter Server Appliance.

d Upgrade vCenter Server. See Chapter 4 Upgrading and Updating vCenter Server for Windows or Chapter 5 Upgrading and Patching the vCenter Server Appliance and Platform Services Controller Appliance.

You can upgrade vCenter Server 5.0 to an embedded or external Platform Services Controller deployment. For vCenter Server 5.1 or 5.5 upgrades, your deployment outcome after upgrade depends upon your initial deployment. For more information on deployment details and how they affect upgrades, see About the vCenter Server 6.0 for Windows Upgrade Process,Upgrading the vCenter Server Appliance, Patching the vCenter Server Appliance and Platform Services Controller Appliance, and vCenter Server Example Upgrade Paths.

6 After upgrading vCenter Server, complete the post-upgrade tasks. Depending on your configuration details before upgrade, you might need to complete some reconfiguration tasks. See Chapter 6 After Upgrading vCenter Server.

7 If you are using vSphere Update Manager, upgrade it. See Chapter 7 Upgrading Update Manager.

8 Upgrade your ESXi hosts.

   a Review the best practices for upgrading and verify that your system meets the upgrade requirements. See Best Practices for ESXi Upgrades and ESXi Requirements.

   b Determine the ESXi upgrade option to use. See Upgrade Options for ESXi 6.0.

   c Determine where you want to locate and boot the ESXi installer. See Media Options for Booting the ESXi Installer. If you are PXE-booting the installer, verify that your network PXE infrastructure is properly set up. See PXE Booting the ESXi Installer.

   d Upgrade ESXi.

      - Using vSphere Update Manager to Perform Orchestrated Host Upgrades
      - Installing or Upgrading Hosts by Using a Script
      - Using vSphere Auto Deploy to Reprovision Hosts
      - Upgrading Hosts by Using esxcli Commands
      - Upgrade Hosts Interactively

9 After upgrading ESXi hosts, you must reconnect the hosts to the vCenter Server and reapply the licenses. See Chapter 10 After You Upgrade ESXi Hosts.

10 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 and Configure Syslog on ESXi Hosts.

11 Upgrade your VMs and virtual appliances, manually or by using vSphere Update Manager, to perform an orchestrated upgrade. See Chapter 11 Upgrading Virtual Machines and VMware Tools.

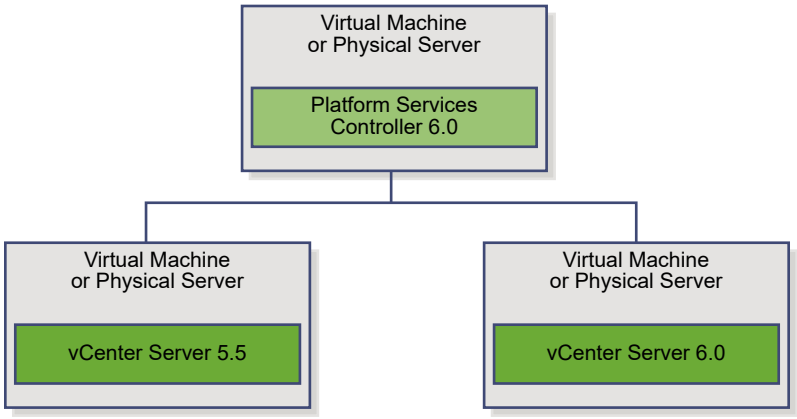
## Mixed-Version Transitional Environments During vCenter Server Upgrades

You can upgrade a vCenter Single Sign-On instance that is deployed on a separate virtual machine or physical server from vCenter Server to an externally deployed Platform Services Controller 6.0 while leaving the vCenter Server instances that are using it at version 5.5.

If you upgrade an externally deployed vCenter Single Sign-On instance to an externally deployed Platform Services Controller 6.0, the vCenter Server 5.5 instances that were using the vCenter Single Sign-On instance are not affected. The vCenter Server 5.5 instances continue to operate with the upgraded Platform Services Controller as they did before the upgrade without any problems or required reconfiguration. vCenter Server 5.5 instances continue to be visible to vSphere Web Client 5.5, though vCenter Server 6.0 instances are not visible to vSphere Web Client 5.5.

Mixed-version transitional behavior is the same for vCenter Single Sign-On instances deployed in vCenter Server 5.5 for Windows environments and in vCenter Server Appliance environments.

Figure 1-5. Mixed-Version Environment




**Note** Mixed-version environments are not supported for production. They are recommended only during the period when an environment is in transition between vCenter Server versions.

If you upgrade an external vCenter Single Sign-On and at least one instance of vCenter Server to version 6.0 while leaving other instances of vCenter Server at version 5.5, expect these results:

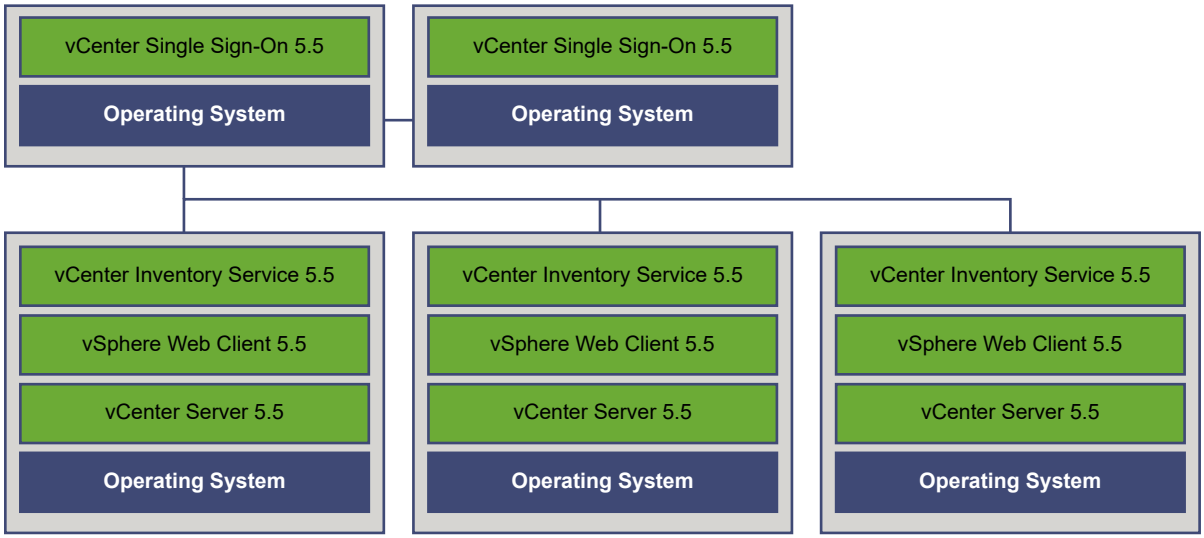
- Linked Mode no longer functions.
- vCenter Server 5.5 instances continue to operate with the upgraded Platform Services Controller as they did before the upgrade without any problems or required reconfiguration.
- In a vCenter Server mixed-version 5.5 and 6.0 environment, a vSphere Web Client 6.0 instance shows vCenter Server 5.5 instances.
- vSphere Web Client 5.5 shows vCenter Server instances only, not 6.0 instances.

If you upgrade all vCenter Server 5.5 instances to version 6.0 and the distributed vCenter Single Sign-On instance to an external Platform Services Controller, none of the vCenter Server instances are affected. They continue operating with the Platform Services Controller as they did before the upgrade without any problems or required action.

The only action required for a mixed-version 5.5 and 6.0 environment after upgrade is a restart of any legacy vSphere Web Client instances if they will be used to view vCenter Server 5.5 instances that are not yet upgraded.

Figure 1-6. Example Deployment Before Upgrade Begins

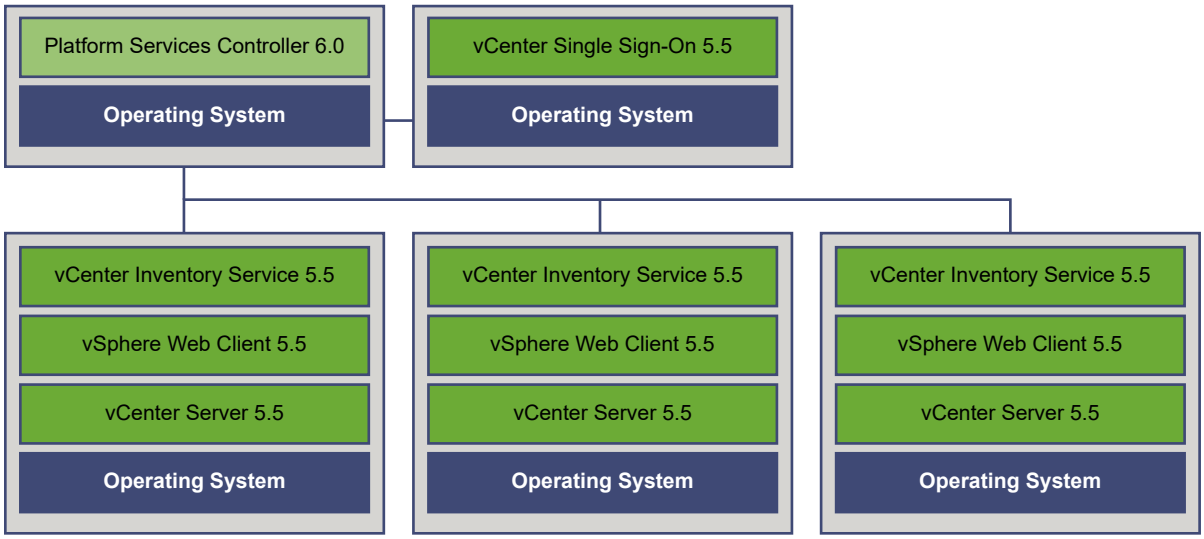
**Transitional Upgrade Environment: Starting Configuration**




For example, a deployment with three vCenter Server 5.5 instances and two external vCenter Single Sign-On instances must be upgraded one instance at a time to version 6.0.

Figure 1-7. Example Deployment in Transition at Step 1

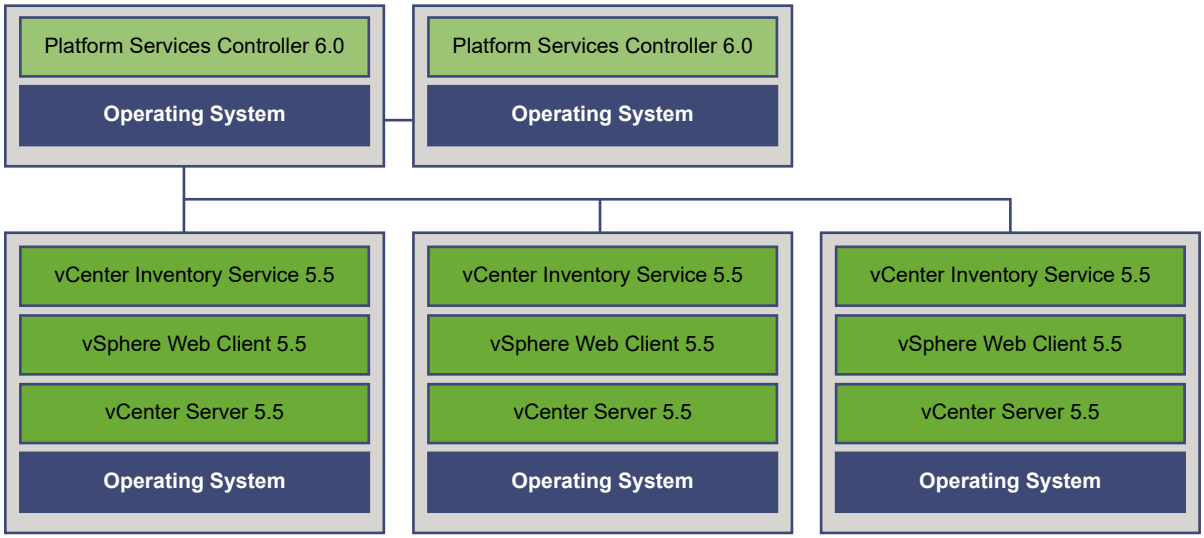
**Transitional Upgrade Environment: Step 1**




Upgrading the first external vCenter Single Sign-On instance to an external Platform Services Controllerhas no impact on the vCenter Server 5.5 instances except that Linked Mode no longer functions.

Figure 1-8. Example Deployment in Transition at Step 2

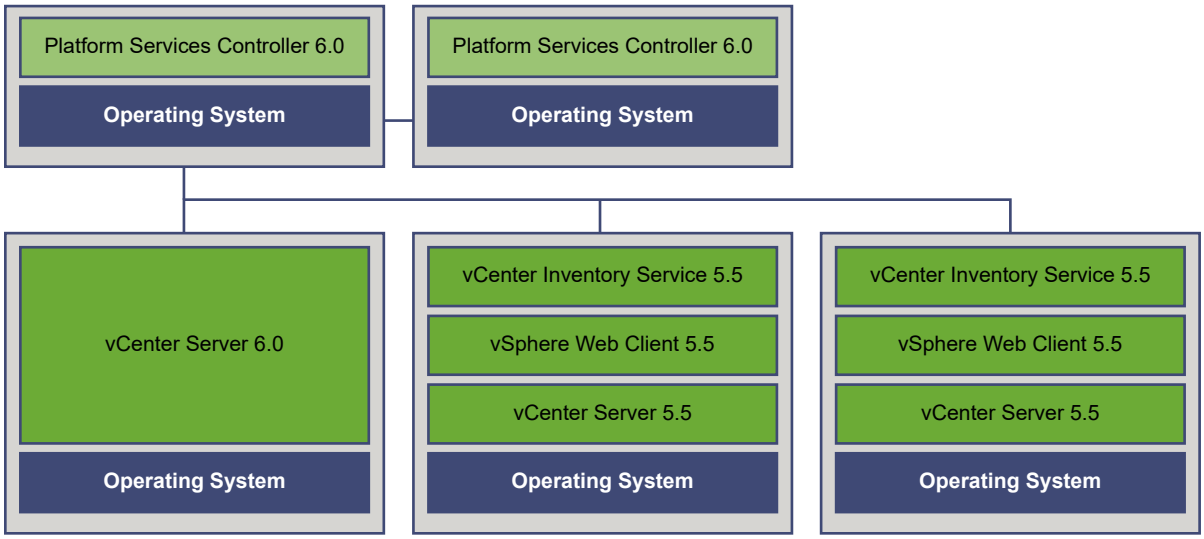
**Transitional Upgrade Environment: Step 2**




Upgrading the second external vCenter Single Sign-On instance to an external Platform Services Controllerhas no impact on the behavior of the vCenter Server 5.5 instances.

Figure 1-9. Example Deployment in Transition at Step 3

**Transitional Upgrade Environment: Step 3**

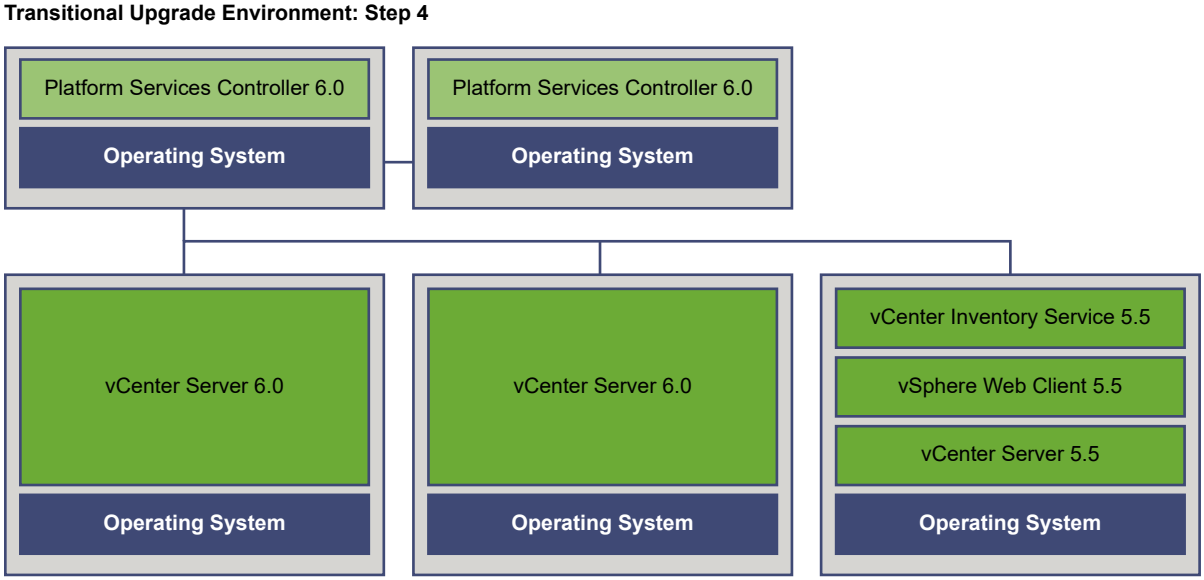



After upgrading the first vCenter Server instance to 6.0, changes occur in the connectivity between the vCenter Server instances.

- The two remaining vSphere Web Client 5.5 instances can no longer view the newly upgraded vCenter Server 6.0 instance after it joins the Platform Services Controller instance.
- The vSphere Web Client 5.5 instances can still view the vCenter Server 5.5 instances after the vSphere Web Client 5.5 instances are restarted.

- The vSphere Web Client 6.0 instance that is part of the newly upgraded vCenter Server 6.0 instance can view the vCenter Server 5.5 and vCenter Server 6.0 instance.

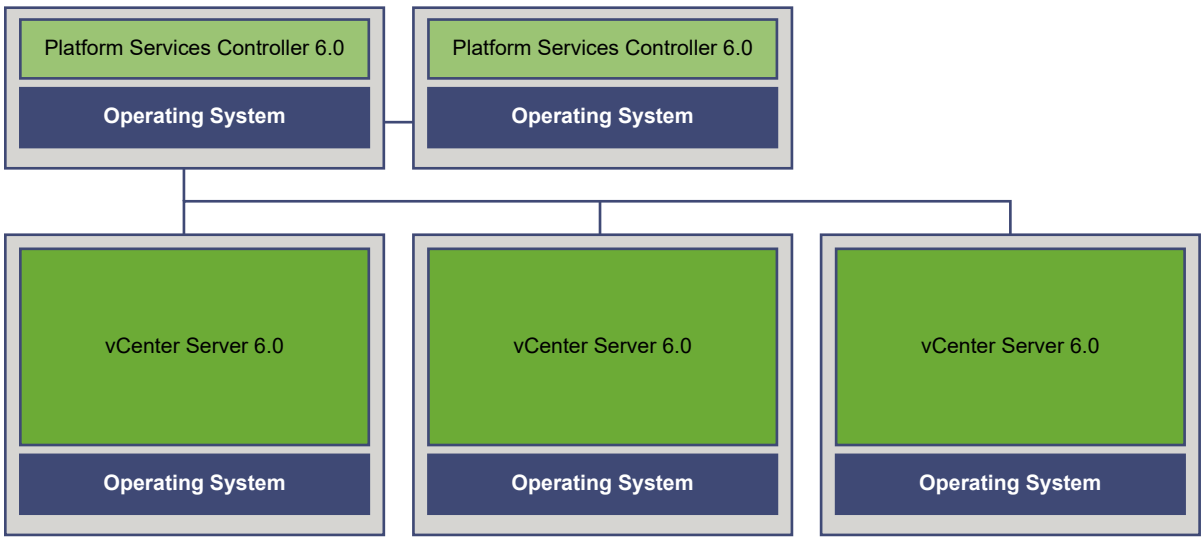
Figure 1-10. Example Deployment in Transition at Step 4




After upgrading the second vCenter Server instance to 6.0, further changes occur in the connectivity between the vCenter Server instances:

- Linked Mode functionality is replaced by Enhanced Linked Mode functionality between the newly upgraded vCenter Server 6.0 instances after they are joined to the Platform Services Controller.
- The remaining vSphere Web Client 5.5 instance can no longer view the vCenter Server 6.0 instances.
- The vSphere Web Client 5.5 instance can still view the vCenter Server 5.5 instance after the vSphere Web Client 5.5 instance is restarted.
- The vSphere Web Client 6.0 instances that are part of the newly upgraded vCenter Server 6.0 instances can view the vCenter Server 5.5 and vCenter Server 6.0 instances.

Figure 1-11. Example Deployment in Transition at Step 5 with Upgrade Complete




After upgrading the third and final vCenter Server instance to 6.0, all the vCenter Server instances are connected with vCenter Server 6.0 functionality.

- Linked Mode functionality is replaced by Enhanced Linked Mode functionality between all the vCenter Server 6.0 instances after they are joined to the Platform Services Controller.
- The vSphere Web Client 6.0 instances can view all the vCenter Server 6.0 instances.

vCenter Server 5.5 to 6.0 Transitional Upgrade Environments (https://vmwaretv.vmware.com/media/t/1_orp6ck9v)

## Upgrading to vSphere License Service

In vSphere 5.x, the license management and reporting functions resides in individual vCenter Server systems. vSphere 6.0 introduces the License Service included in the Platform Services Controller. The License Service provides common license inventory and management capabilities to the vCenter Server systems that are registered to a Platform Services Controller or multiple Platform Services Controllers that are joined in one vCenter Single Sign-On domain.

During the upgrade of the vCenter Server systems that are connected to a Platform Services Controller, their licensing data is transferred to the License Service. The licensing data includes the available licenses and license assignments for hosts, vCenter Server systems, Virtual SAN clusters, and other products that you use with vSphere.

After the upgrade of the vCenter Server systems completes, the License Services stores the available licenses and manages the license assignments for the entire vSphere environment. If your vSphere environment consists of multiple Platform Services Controllers joined in one vCenter Single Sign-On domain, the License Service in every Platform Services Controller contains a replica of the licensing data for the entire environment.

For more information about the License Service and managing licenses in vSphere, see *vCenter Server and Host Management*.

## Differences Between vSphere Upgrades and Updates

vSphere products distinguish between upgrades, which make major changes to the software, and updates, which make smaller changes to the software.

VMware product versions are numbered with two digits, for example, vSphere 6.0. A release that changes either digit, for example, from 5.5 to 6.0, or from 5.1 to 5.5, involves major changes in the software, and requires an upgrade from the previous version. A release that makes a smaller change, requiring only an update, is indicated by an update number, for example, vSphere 6.0 Update 1.

When you upgrade an ESXi host, some host configuration information is preserved in the upgraded version, and the upgraded host, after rebooting, can join a vCenter Server instance that has been upgraded to the same level. Because updates and patches do not involve major changes to the software, host configuration is not affected. For more details, see Upgrade or Update a Host with Image Profiles

# How vCenter Single Sign-On Affects Upgrades

If you upgrade a Simple Install environment to a vCenter Server 6 embedded deployment, upgrade is seamless. If you upgrade a custom installation, the vCenter Single Sign-On service is part of the Platform Services Controller after the upgrade. Which users can log in to vCenter Server after an upgrade depends on the version that you are upgrading from and the deployment configuration.

As part of the upgrade, you can define a different vCenter Single Sign-On domain name to be used instead of vsphere.local.

## Upgrade Paths

The result of the upgrade depends on what installation options you had selected, and what deployment model you are upgrading to.

Table 1-1. Upgrade Paths

| Source | Result |
| --- | --- |
| vSphere 5.5 and earlier Simple Install | vCenter Server with embedded Platform Services Controller. |
| vSphere 5.5 and earlier Custom Install | If vCenter Single Sign-On was on a different node than vCenter Server, an environment with an external Platform Services Controller results.<br>If vCenter Single Sign-On was on the same node as vCenter Server, but other services are on different nodes, an environment with an embedded Platform Services Controller results.<br>If the custom installation included multiple replicating vCenter Single Sign-On servers, an environment with multiple replicating Platform Services Controller instances results. |

## Who Can Log In After Upgrade of a Simple Install

If you upgrade an environment that you provisioned using the Simple Install option, the result is always an installation with an embedded Platform Services Controller. Which users are authorized to log in depends on whether the source environment includes vCenter Single Sign-On.

Table 1-2. Login Privileges After Upgrade of Simple Install Environment

| Source version | Login access for | Notes |
|---|---|---|
| vSphere 5.0 | Local operating system users<br>administrator@vsphere.local | You might be prompted for the administrator of the root folder in the vSphere inventory hierarchy during installation because of changes in user stores.<br>If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source. |
| vSphere 5.1 | Local operating system users<br>administrator@vsphere.local<br>Admin@SystemDomain | Starting with vSphere 5.5, vCenter Single Sign-On supports only one default identity source.<br>You can set the default identity source.<br>See the *vSphere Security* documentation.<br>Users in a non-default domain can specify the domain when they log in (*DOMAIN**user* or user@*DOMAIN*). |
| vSphere 5.5 | administrator@vsphere.local or the administrator of the domain that you specified during upgrade.<br>All users from all identity sources can log in as before. | |

If you upgrade from vSphere 5.0, which does not include vCenter Single Sign-On, to a version that includes vCenter Single Sign-On, local operating system users become far less important than the users in a directory service such as Active Directory. As a result, it is not always possible, or even desirable, to keep local operating system users as authenticated users.

## Who Can Log In After Upgrade of a Custom Installation

If you upgrade an environment that you provisioned using the Custom Install option, the result depends on your initial choices:

- If vCenter Single Sign-On was on the same node as the vCenter Server system, the result is an installation with an embedded Platform Services Controller.
- If vCenter Single Sign-On was on a different node than the vCenter Server system, the result is an installation with an external Platform Services Controller.
- If you upgrade from vSphere 5.0, you can select an external or embedded Platform Services Controller as part of the upgrade process.

Login privileges after the upgrade depend on several factors.

Table 1-3. Login Privileges After Upgrade of Custom Install Environment

| Source version | Login access for | Notes |
|---|---|---|
| vSphere 5.0 | vCenter Single Sign-On recognizes local operating system users for the machine where the Platform Services Controller is installed, but not for the machine where vCenter Server is installed.<br>**Note** Using local operating users for administration is not recommended, especially in federated environments.<br>administrator@vsphere.local can log in to vCenter Single Sign-On and each vCenter Server instance as an administrator user. | If your 5.0 installation supported Active Directory users, those users no longer have access after the upgrade. You can add the Active Directory domain as an identity source. |
| vSphere 5.1 or vSphere 5.5 | vCenter Single Sign-On recognizes local operating system users for the machine where the Platform Services Controller is installed, but not for the machine where vCenter Server is installed.<br>**Note** Using local operating users for administration is not recommended, especially in federated environments.<br>administrator@vsphere.localcan log in to vCenter Single Sign-On and each vCenter Server instance as an administrator user.<br>For upgrades from vSphere 5.1 Admin@SystemDomain has the same privileges as administrator@vsphere.local. | Starting with vSphere 5.5, vCenter Single Sign-On supports only one default identity source.<br>You can set the default identity source.<br>See the *vSphere Security* documentation.<br>Users in a non-default domain can specify the domain when they log in (*DOMAIN**user* or user@*DOMAIN*). |

# 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.

# 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 http://kb.vmware.com/kb/2108548.

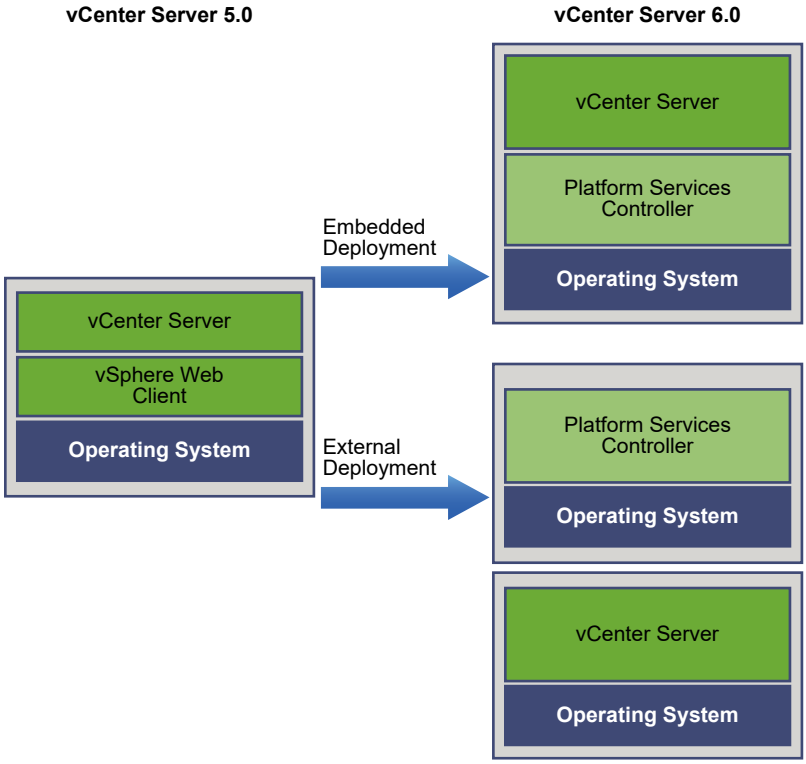
# vCenter Server Example Upgrade Paths

Your initial vCenter Server 5.x configuration determines your upgrade and 6.0 configuration options.

Example upgrade paths demonstrate some of common starting configurations before vCenter Server upgrade and their expected configuration outcomes after vCenter Server upgrade.

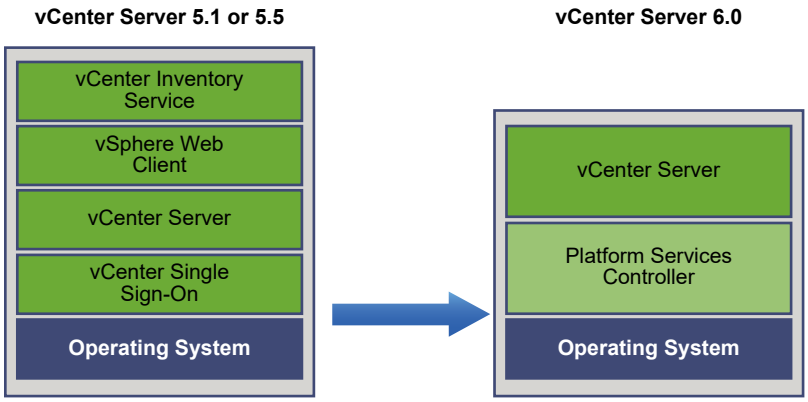
If you are currently using vCenter Server 5.0, you do not have any common services configured. You have a choice of upgrading to vCenter Server with an embedded Platform Services Controller or upgrading to vCenter Server with an external Platform Services Controller.

Figure 1-12. vCenter Server 5.0 Deployment Choices for Upgrade



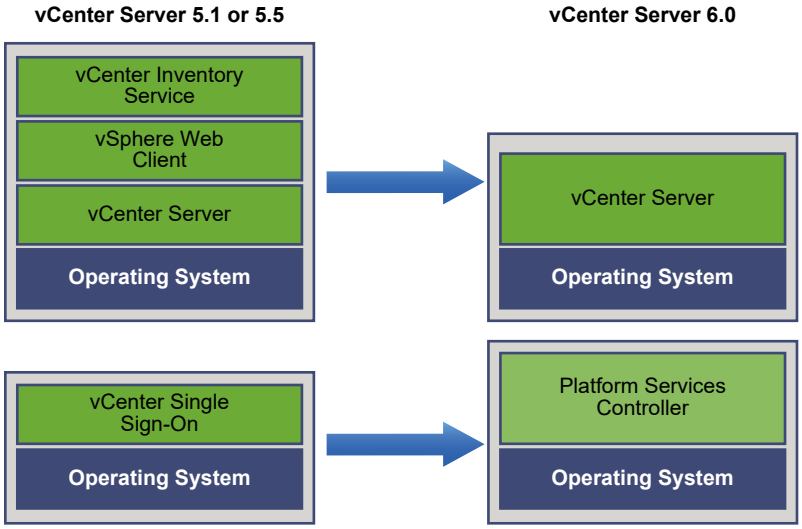

If you have a simple installation with all vCenter Server 5.1 or 5.5 components on the same system, the vCenter Server 6.0 software upgrades your system to vCenter Server with an embedded Platform Services Controller instance. The software upgrades your vCenter Server common services such as vCenter Single Single-On in the Platform Services Controller instance. The rest of the vCenter Server components, such as vSphere Web Client Inventory Service, are upgraded to 6.0 as part of the vCenter Server group of services. The software upgrades vCenter Server and all its services in the correct order to the same version.

Figure 1-13. vCenter Server 5.1 or 5.5 with Embedded vCenter Single Sign-On Deployment Before and After Upgrade



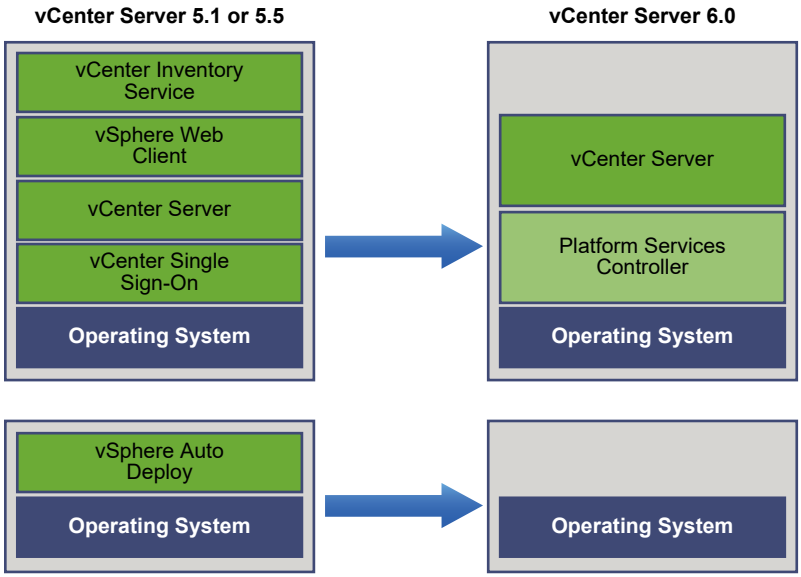
If you have a custom vCenter Server 5.1 or 5.5 environment with an externally deployed vCenter Single Sign-On, the vCenter Server 6.0 software upgrades your deployment to vCenter Server with an external Platform Services Controller instance.

Figure 1-14. vCenter Server 5.1 or 5.5 with Externally Deployed vCenter Single Sign-On Before and After Upgrade




If your configuration includes a vSphere Auto Deploy server, the upgrade process upgrades it when upgrading the associated vCenter Server instance. You cannot use a vSphere Auto Deploy server that was included with an earlier version of the product in conjunction with vCenter Server 6.0. If your vSphere Auto Deploy server is running on a remote system, it is upgraded and migrated to the same system as vCenter Server during the upgrade process.

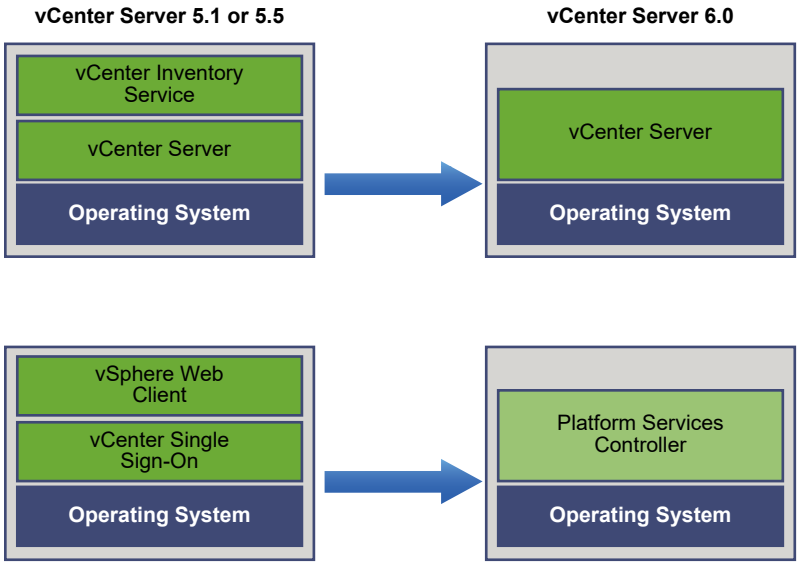
Figure 1-15. vCenter Server 5.1 or 5.5 with Remote vSphere Auto Deploy Server Before and After Upgrade



For example, if your vCenter Server is part of vCenter Server Appliance, and you installed the vSphere Auto Deploy server on a Windows machine, the upgrade process migrates the vSphere Auto Deploy server to the same location as your vCenter Server Appliance. Any settings are migrated to the new location. However, you must reconfigure your ESXi hosts to point to the new vSphere Auto Deploy location. See Reconfigure Migrated vCenter Server Services After Upgrade

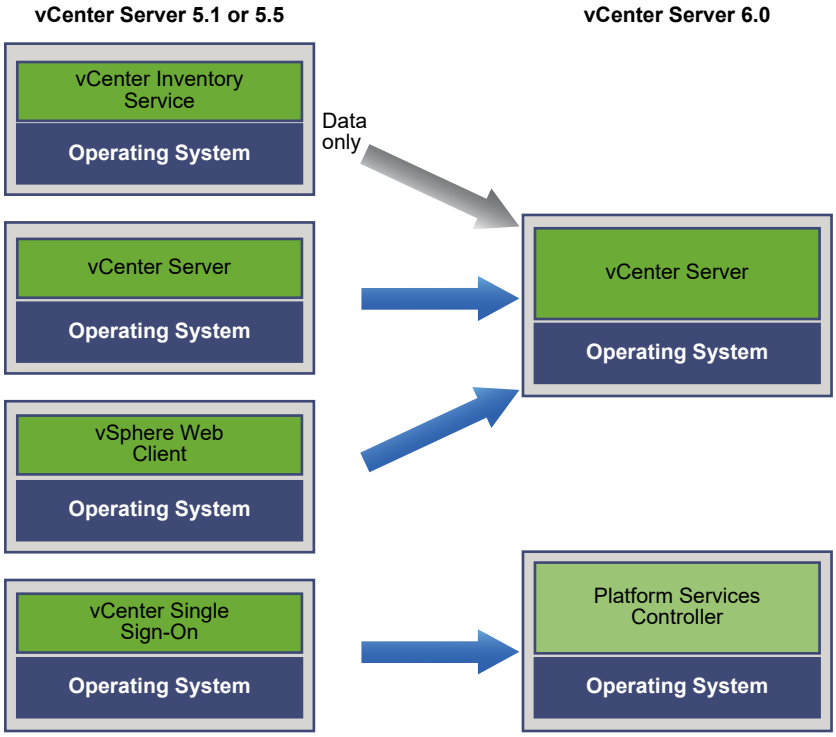
If your configuration includes a remotely deployed vSphere Web Client, it is upgraded along with the vCenter Server instance to which it is registered and migrated to the same location as the vCenter Server instance.

**Figure 1-16. vCenter Server 5.1 or 5.5 with Remote vSphere Web Client and vCenter Signle Sign-On Before and After Upgrade**




Only the vCenter Single Sign-On instance remains remotely deployed as part of the the Platform Services Controller instance after upgrade to vCenter Server 6.0. If all vCenter Server components are deployed remotely, all are migrated to the vCenter Server location during the upgrade except vCenter Single Sign-On. While Inventory Service data is migrated to the vCenter Server location, the legacy version is no longer used and must be uninstalled manually. See Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0

Figure 1-17. vCenter Server 5.1 or 5.5 with All Remote Components Before and After Upgrade




If you have multiple systems configured for high availability, vCenter Server enables you to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process.

If you have a multisite setup configured with replication, you can use vCenter Server to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process.

Upgrading vCenter Server from 5.0 to 6.0 (https://vmwaretv.vmware.com/media/t/1_ih7nmi18)

Upgrading vCenter Server from 5.1 or 5.5 to 6.0 (https://vmwaretv.vmware.com/media/t/1_vs0qr73b)

For more information on mixed version transitional environments, see Mixed-Version Transitional Environments During vCenter Server Upgrades

# Upgrade Requirements

2

To upgrade vCenter Server and ESXi instances, your systems must meet specific requirements.

This chapter includes the following topics:



## vCenter Server Upgrade Compatibility

The upgrade to vCenter Server 6.0 affects other software components of the data center.

Table 2-1. Upgrading vCenter Server and Related VMware Products and Components summarizes how upgrading vCenter Server can affect your data center components.

vCenter Server 6.0 can manage ESXi 5.x hosts in the same cluster with ESXi 6.0 hosts, but not ESX 4.x or ESXi 4.x hosts.

You cannot upgrade to vCenter Server 6.0 from vCenter Server 4.x or earlier. You must first upgrade to vCenter Server 5.x.

Table 2-1. Upgrading vCenter Server and Related VMware Products and Components

| Product or Component | Compatibility |
|---|---|
| vCenter Server | Verify support for the upgrade path from your current version of vCenter Server to your planned upgrade version. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. |
| vCenter Server database | Verify that your database is supported for the vCenter Server version that you are upgrading to. Upgrade the database if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.<br><br>**Note** vCenter Server Appliance for vCenter Server 6.0 uses PostgreSQL for the embedded database. For external databases, vCenter Server Appliance supports only Oracle databases, in the same versions shown in the VMware Product Interoperability Matrix for the version of vCenter Server that you are upgrading to. |
| vSphere Web Client | Verify that your vSphere Web Client works with the vCenter Server version that you are upgrading to. For best performance and compatibility, upgrade your vSphere Web Client to the same version as your vCenter Server. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. |
| ESX and ESXi hosts | Verify that your ESX or ESXi host works with the vCenter Server version that you are upgrading to. Upgrade if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. |
| VMware Virtual Machine File System (VMFS) volumes | You can continue to use existing VMFS3 datastores, but you cannot create new VMFS3 datastores. If you have VMFS3 datastores, upgrade them to VMFS5. For information on upgrading your VMFS volumes, see the *vSphere Storage* document. |
| Virtual machines | Upgrade options depend on your current version. See Chapter 11 Upgrading Virtual Machines and VMware Tools. |
| VMware Tools | Upgrade options depend on your current version. See the information about upgrading VMware Tools in Chapter 11 Upgrading Virtual Machines and VMware Tools. |
| Auto Deploy | To ensure compatibility and best performance, when you upgrade to vCenter Server 6.0, use Auto Deploy to upgrade ESXi hosts to the same version. |

# vCenter Server for Windows Requirements

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

- Synchronize the clocks on all machines running the vCenter Server 5.x services. See Synchronizing Clocks on the vSphere Network.
- Verify that the system network name of the machines running vCenter Server 5.x services are valid, and are reachable from other machines in the network.
- 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.

- 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)**
- 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-Upgrade Checker

When you upgrade vCenter Server and the Platform Services Controller, the installer does a pre-upgrade check, for example, to verify that enough space is available on the virtual machine or physical server where you are upgrading 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 upgrade, 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 upgrade process.

The pre-upgrade 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
- vCenter Server 5.x services

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

## vCenter Server for Windows Storage Requirements

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

The storage requirements per folder depend on the vCenter Server 5.x services deployed on the machine, the upgrade deployment model, and the size of your vSphere 5.x inventory. The installer dynamically calculates the storage requirement during the upgrade, and verifies that the machine has sufficient free disk space before proceeding with the upgrade.

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. The following table lists the absolute minimum disk space requirements for the different deployment models. The requirements change depending on the installed vCenter Server 5.x services and the vSphere 5.x inventory size.

**Table 2-2. 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 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 2-3. Minimum Recommended Hardware Requirements for Installing vCenter Server and Platform Services Controller on Windows

| | Platform Services Controller | vCenter Server with an Embedded or External Platform Services Controller for a Tiny Environment (up to 10 Hosts, 100 Virtual Machines) | vCenter Server with an Embedded or External Platform Services Controller for a Small Environment (up to 100 Hosts, 1000 Virtual Machines) | vCenter Server with an Embedded or External Platform Services Controller for a Medium Environment (up to 400 Hosts, 4,000 Virtual Machines) | vCenter Server with an Embedded or External Platform Services Controller for a 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 |

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 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 http://kb.vmware.com/kb/2091273.

## 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. A larger installation requires a supported external database for the size of the environment.

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 upgrade the vCenter Server Appliance on an ESXi host 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.

## 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 2-4. Hardware Requirements for VMware vCenter Server Appliance and Platform Services Controller Appliance**

| Resources | Platform Services Controller Appliance | vCenter Server Appliance with an Embedded or External Platform Services Controller for a Tiny Environment (up to 10 Hosts, 100 Virtual Machines) | vCenter Server Appliance with an Embedded or External Platform Services Controller for a Small Environment (up to 100 Hosts, 1,000 Virtual Machines) | vCenter Server Appliance with an Embedded or External Platform Services Controller for a Medium Environment (up to 400 Hosts, 4,000 Virtual Machines) | vCenter Server Appliance with an Embedded or External Platform Services Controller for a 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 |

## 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 2-5. 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 upgraded only on hosts that are running ESXi version 5.0 or later.

You can upgrade 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.

## Required Ports for vCenter Server and Platform Services Controller

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 denylisted, 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 2-6. Ports Required for Communication Between Components

| Port | Protocol | Description | Required for | Used for Node-to-Node Communication |
|---|---|---|---|---|
| 22 | TCP | System port for SSHD.<br>**Important** This port must be open during the upgrade of the appliance. The upgrade process establishes an SSH connection to transfer the data from the existing to the new appliance. | Appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | No |
| 80 | TCP | 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.<br>WS-Management (also requires port 443 to be open).<br>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.<br>**Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows. | Windows installations and appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | No |
| 88 | TCP | Active Directory server. This port must be open for host to join Active Directory. If you use native Active Directory, the port must be open on both vCenter Server and the Platform Services Controller. | Windows installations and appliance deployments of Platform Services Controller | No |

Table 2-6. Ports Required for Communication Between Components (continued)

| Port | Protocol | Description | Required for | Used for Node-to-Node Communication |
|---|---|---|---|---|
| 389 | TCP/UDP | 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.<br>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. | Windows installations and appliance deployments of Platform Services Controller | ■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to Platform Services Controller |
| 443 | TCP | 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.<br>The vCenter Server system also uses port 443 to monitor data transfer from SDK clients.<br>This port is also used for the following services:<br>■ WS-Management (also requires port 80 to be open)<br>■ Third-party network management client connections to vCenter Server<br>■ Third-party network management clients access to hosts<br>**Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows. | Windows installations and appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | ■ vCenter Server to vCenter Server<br>■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to vCenter Server |
| 514 | TCP/UDP | vSphere Syslog Collector port for vCenter Server on Windows and vSphere Syslog Service port for vCenter Server Appliance<br>**Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows. | Windows installations and appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | No |

Table 2-6. Ports Required for Communication Between Components (continued)

| Port | Protocol | Description | Required for | Used for Node-to-Node Communication |
|---|---|---|---|---|
| 636 | TCP | vCenter Single Sign-On LDAPS | Windows installations and appliance deployments of Platform Services Controller | vCenter Server to Platform Services Controller |
| 902 | TCP/UDP | 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.<br>Port 902 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this port to display virtual machine consoles<br>**Important** You can change this port number during the vCenter Server installations on Windows. | Windows installations and appliance deployments of vCenter Server | No |
| 1514 | TCP/UDP | vSphere Syslog Collector TLS port for vCenter Server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance<br>**Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows. | Windows installations and appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | No |
| 2012 | TCP | Control interface RPC for vCenter Single Sign-On | Windows installations and appliance deployments of Platform Services Controller | ■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to vCenter Server<br>■ Platform Services Controller to Platform Services Controller |
| 2014 | TCP | RPC port for all VMCA (VMware Certificate Authority) APIs<br>**Important** You can change this port number during the Platform Services Controller installations on Windows. | Windows installations and appliance deployments of Platform Services Controller | ■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to vCenter Server |

Table 2-6. Ports Required for Communication Between Components (continued)

| Port | Protocol | Description | Required for | Used for Node-to-Node Communication |
|---|---|---|---|---|
| 2020 | TCP/UDP | Authentication framework management<br>**Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows. | Windows installations and appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | ■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to vCenter Server |
| 5480 | TCP | Appliance Management Interface<br>Open endpoint serving all HTTPS, XMLRPS and JSON-RPC requests over HTTPS. | Appliance deployments of<br>■ vCenter Server<br>■ Platform Services Controller | No |
| 6500 | TCP/UDP | ESXi Dump Collector port<br>**Important** You can change this port number during the vCenter Server installations on Windows. | Windows installations and appliance deployments of vCenter Server | No |
| 6501 | TCP | Auto Deploy service<br>**Important** You can change this port number during the vCenter Server installations on Windows. | Windows installations and appliance deployments of vCenter Server | No |
| 6502 | TCP | Auto Deploy management<br>**Important** You can change this port number during the vCenter Server installations on Windows. | Windows installations and appliance deployments of vCenter Server | No |
| 7444 | TCP | Secure Token Service | Windows installations and appliance deployments of Platform Services Controller | ■ vCenter Server to Platform Services Controller<br>■ Platform Services Controller to vCenter Server |
| 9443 | TCP | vSphere Web Client HTTPS | Windows installations and appliance deployments of vCenter Server | No |

Table 2-6. Ports Required for Communication Between Components (continued)

| Port | Protocol | Description | Required for | Used for Node-to-Node Communication |
|---|---|---|---|---|
| 11711 | TCP | vCenter Single Sign-On LDAP | - | For backward compatibility with vSphere 5.5 only.<br>vCenter Single Sign-On 5.5 to Platform Services Controller 6.0 |
| 11712 | TCP | vCenter Single Sign-On LDAPS | - | For backward compatibility with vSphere 5.5 only.<br>vCenter Single Sign-On 5.5 to Platform Services Controller 6.0 |

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.

# vCenter Server Database Configuration Notes

After you select a supported database type, make sure you understand any special configuration requirements.

Table 2-7. Configuration Notes for Databases Supported with vCenter Server 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 2-7. Configuration Notes for Databases Supported with vCenter Server.

**Note** vSphere Update Manager also requires a database. Use separate databases for vCenter Server and vSphere Update Manager.

vCenter Server databases require a UTF code set.

Table 2-7. 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.<br>**Important** If you use the embedded PostgreSQL database, uninstalling vCenter Server on Windows, uninstalls the embedded database, and all data is lost.<br>When you upgrade vCenter Server 5.x to vCenter Server 6.0, the bundled Microsoft SQL Server Express database is migrated to PostgreSQL. |
| Microsoft SQL Server 2008 R2 SP2 or higher | Ensure that the machine has a valid ODBC DSN entry.<br>**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.<br>**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.<br>**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.<br>After you complete the vCenter Server installation, apply the latest patch to the Oracle client and server. |

# 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.

## 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 the topic "Set the Scratch Partition from the vSphere Web Client" in the *vSphere Installation and Setup* documentation.

Due to the I/O sensitivity of USB and SD devices the installer does not create a scratch partition on these devices. 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 http://kb.vmware.com/kb/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 2-8. 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. See also the technical papers on vSphere performance at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-perfbest-practices-vsphere6-0-white-paper.pdf.

Table 2-9. 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.<br>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.<br>Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines.<br>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. |

Table 2-9. Recommendations for Enhanced Performance (continued)

| System Element | Recommendation |
|---|---|
| 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.<br><br>**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 2-10. 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. |

Table 2-10. Incoming Firewall Connections (continued)

| Service | Port | Comment |
|---|---|---|
| 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.<br>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 2-11. 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. |

Table 2-11. Outgoing Firewall Connections (continued)

| Service | Port | Comment |
|---|---|---|
| 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. |
| WOL | 9 (UDP) | Used by Wake on LAN. |
| 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. |

Table 2-11. Outgoing Firewall Connections (continued)

| Service | Port | Comment |
|---|---|---|
| VMware vCenter Agent | 902 (UDP) | vCenter Server agent. |
| vsanvp | 8080 (TCP) | Used for Virtual SAN Vendor Provider traffic. |

# 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.

# 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 2-12. 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.<br>Mozilla Firefox 34 and later.<br>Google Chrome 39 and later. |
| Mac OS | Mozilla Firefox 34 and later.<br>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 2-13. 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 2-14. vSphere Client Minimum Hardware Requirements and Recommendations

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

Table 2-14. vSphere Client Minimum Hardware Requirements and Recommendations (continued)

| vSphere Client Hardware | Requirements and Recommendations |
|---|---|
| Disk Storage | 1.5GB free disk space for a complete installation, which includes the following components:<br>■ Microsoft .NET 2.0 SP2<br>■ Microsoft .NET 3.0 SP2<br>■ Microsoft .NET 3.5 SP1<br>■ Microsoft Visual J#<br>Remove any previously installed versions of Microsoft Visual J# on the system where you are installing the vSphere Client.<br>■ vSphere Client<br>If you do not have any of these components already installed, you must have 400MB free on the drive that has the `%temp%` directory.<br>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 2-15. TCP and UDP Ports

| Port | Purpose | Traffic Type |
|---|---|---|
| 443 (Default) | HTTPS access<br>vSphere Client access to vCenter Server<br>vSphere Client access to ESXi hosts<br>vSphere Client access to vSphere Update Manager | Incoming TCP to the ESXi host |
| 902 (Default) | vSphere Client access to virtual machine consoles | Incoming TCP to the ESXi host, outgoing TCP from the ESXi host, outgoing UDP from the ESXi host |

# 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 2-16. 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 and configuring syslog and a syslog server and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

# Before Upgrading vCenter Server 3

Ensure that your system is prepared for vCenter Server upgrade by verifying compatibility and completing any necessary database, networking, or other preparation tasks.

This chapter includes the following topics:



## Verify Basic Compatibility Before Upgrading vCenter Server

Verify that all components meet basic compatibility requirements before upgrading vCenter Server.

Upgrading the operating system of a vCenter Single Sign-On 5.1 machine from Windows 2003 to Windows 2008 to meet the operating system requirements may result in symptoms similar to knowledge base article 2036170.

**Prerequisites**

Verify that your system meets the hardware and software requirements. See vCenter Server for Windows Requirements and vCenter Server Appliance Requirements

If you have solutions or plug-ins, check the VMware Product Interoperability Matrix. See http://www.vmware.com/resources/compatibility/sim/interop_matrix.php

Procedure

1. The installation path of the previous version of vCenter Server must be compatible with the installation requirements for Microsoft Active Directory Application Mode (ADAM/AD LDS).

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation marks (!), pound signs (#), at signs (@), or percentage signs (%).

   If your previous version of vCenter Server does not meet this requirement, you must perform a fresh installation of vCenter Server.
2. Verify that the vCenter Server system is not an Active Directory primary or backup domain controller.
3. Update any ESX/ESXi 4.1 hosts to version 5.x.
4. If you have ESX 4.x hosts that you choose not to upgrade, you must remove them from the vCenter Server inventory.
5. If the vCenter Server 4.x environment that you are upgrading includes Guided Consolidation 4.x, uninstall Guided Consolidation before upgrading to vCenter Server 6.0.

# 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.

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.

# Prepare Oracle Database Before Upgrading to vCenter Server 6.0

Ensure that your Oracle database meets requirements, that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before upgrading vCenter Server.

### Prerequisites

Verify that you have confirmed basic upgrade interoperability before preparing your Oracle database for upgrading vCenter Server. See vCenter Server for Windows Database Requirements and vCenter Server Appliance Database Requirements.

Verify that you have backed up your database. For information about backing up the vCenter Server database, see the Oracle documentation.

To set database permissions correctly, see Database Permission Requirements for vCenter Server

### Procedure

1. Verify that your database meets the upgrade requirements. If necessary, upgrade the database to a supported version.
2. If your database server is not supported by vCenter Server, perform a database upgrade to a supported version or import your database into a supported version.
3. If your existing database is Oracle, and you want to upgrade to a newly supported Oracle database, such as Oracle 11g, upgrade your Oracle database before upgrading vCenter Server.

   You do not need to perform a fresh installation of vCenter Server if your existing database is Oracle.

   For example, you can upgrade your existing Oracle 9i database to Oracle 11g or Oracle 12c and upgrade vCenter Server 5.x to vCenter Server 6.0.
4. Verify that passwords are current and not set to expire soon.
5. Ensure that you have login credentials, the database name, and the database server name that the vCenter Server database is to use.

   Look in the ODBC system for the connection name of the database source name for the vCenter Server database.
6. Use the Oracle SERVICE_NAME instead of SID to verify that your Oracle database instance is available.
   - Log in to the database server to read from the alert log: `$ORACLE_BASE/diag//rdbms/$instance_name/$INSTANCE_NAME/trace/alert_$ INSTANCE_NAME.log`.
   - Log in to the database server to read from the Oracle Listener status output.
   - If you have the SQL*Plus client installed, you can use `tnsping` for the vCenter Database instance. If the `tnsping` command does not work the first time, retry it after waiting a few minutes. If retrying does not work, restart the vCenter Database instance on the Oracle server and then retry `tnsping` to ensure it is available.

7 Verify that the JDBC driver file is included in the CLASSPATH variable.

8 Verify that permissions are set correctly.

9 Either assign the DBA role or grant the required permissions to the user.

10 Locate the cleanup_orphaned_data_Oracle.sql script in the ISO image and copy it to the Oracle server.

11 Log in to a SQL*Plus session with the vCenter Server database account.

12 Run the cleanup script.

```
@pathcleanup_orphaned_data_Oracle.sql
```

The cleanup process purges unnecessary and orphaned data that is not used by any vCenter Server component.

13 Make a full backup of the vCenter Server database and the vCenter Inventory Service database.

### Results

Your database is prepared for the vCenter Server upgrade.

### What to do next

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

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

## Prepare Microsoft SQL Server Database Before Upgrading to vCenter Server 6.0

Ensure that your Microsoft SQL Server database meets requirements, that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before upgrading vCenter Server.

To remove the DBO role and migrate all objects in the DBO schema to a custom schema, see the VMware knowledge base article at http://kb.vmware.com/kb/1036331.

Microsoft SQL Server Express is no longer supported for vCenter Server 6.0. The vCenter Server 5.x embedded Microsoft SQL Server Express database is replaced with an embedded PostgreSQL database during the upgrade to vCenter Server 6.0. To upgrade without migrating to the PostgreSQL database, see the VMware knowledge base article http://kb.vmware.com/kb/2109321.

To migrate the vCenter Server database from Microsoft SQL Express to Microsoft full SQL Server, see the VMware knowledge base article at http://kb.vmware.com/kb/1028601.

**Important** You cannot use Integrate Windows for your authentication method if the vCenter Server service is running under the Microsoft Windows built-in system account.

### Prerequisites

Verify that you have confirmed basic upgrade interoperability before preparing your Microsoft SQL Server database for upgrading vCenter Server. See vCenter Server for Windows Database Requirements and vCenter Server Appliance Database Requirements.

Verify that you have backed up your database. For information about backing up the vCenter Server database, see the Microsoft SQL Server documentation.

To set database permissions correctly, see Database Permission Requirements for vCenter Server and Use a Script to Create and Apply a Microsoft SQL Server Database Schema and Roles.

### Procedure

1. Verify that your database meets the upgrade requirements. If necessary, upgrade the database to a supported version.
2. If your database server is not supported by vCenter Server, perform a database upgrade to a supported version or import your database into a supported version.
3. If your existing database is Microsoft SQL Server, and you want to upgrade to a newly supported Microsoft SQL Server database, such as Microsoft SQL Server 2012, upgrade your Microsoft SQL Server database before upgrading vCenter Server.

   You do not need to install a new vCenter Server instance if your existing database is Microsoft SQL Server.

   For example, you can upgrade a Microsoft SQL Server 2005 database to a Microsoft SQL Server 2008 R2-SP2, 2012, or 2014 database and then upgrade vCenter Server 5.0 or later to vCenter Server 6.0.

   When you migrate the database from Microsoft SQL Server 2005 to Microsoft SQL Server 2008 R2-SP2 or later, set the compatibility level of the database to 100.
4. Verify that permissions are set correctly.
5. Verify that passwords are current and not set to expire soon.
6. Verify that JDK 1.6 or later is installed on the vCenter Server machine.
7. Verify that the `sqljdbc4.jar` file is added to the CLASSPATH variable on the machine where vCenter Server is to be upgraded.

   If the `sqljdbc4.jar` file is not installed on your system, the vCenter Server installer installs it.
8. Verify that your system database source name is using the Microsoft SQL Server Native Client 10 or 11 driver.

9 If you choose to remove the DBO role and migrate all objects in the DBO schema to a custom schema, you must grant the required permissions.

   a Grant the required permissions to the vCenter Server user in the vCenter Server database.

   b Grant the required permissions to the user in the MSDB database.

10 Locate the `cleanup_orphaned_data_MSSQL.sql` script in the ISO image and copy it to the Microsoft SQL server.

11 Log in to your database.

   a For Microsoft SQL Server Express, open a command prompt.

   b For Microsoft SQL Server, log in to a Microsoft SQL Server Management Studio session as the vCenter Server database user.

12 For Microsoft SQL Server Express, run the cleanup script.

   sqlcmd -E -S localhost\VIM_SQLEXP -d VIM_VCDB -i *path*cleanup_orphaned_data_MSSQL.sql

13 For Microsoft SQL Server, run the cleanup_orphaned_data_MSSQL.sql contents.

   Make sure that you are connected to the database used by vCenter Server.

   The cleanup script cleans any unnecessary data in your vCenter Server database.

14 Make a full backup of the vCenter Server database and Inventory Service database.

#### Results

Your database is prepared for the vCenter Server upgrade.

## 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*.

#### Prerequisites

To make sure you have the proper roles and permissions before upgrading vCenter Server, update the SQL Server database and users for vCenter Server.

#### 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 roles and apply privileges.

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_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
```

```
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use master
go
grant VIEW SERVER STATE to [vpxuser]
go
GRANT VIEW ANY DEFINITION TO [vpxuser]
go
```

# Prepare PostgreSQL Database Before Upgrading to vCenter Server 6.0

Ensure that your PostgreSQL database meets requirements, that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before upgrading vCenter Server.

For information about backing up the vCenter Server database, see the PostgreSQL documentation.

### Prerequisites

Verify that you have confirmed basic upgrade interoperability before preparing your PostgreSQL database for upgrading vCenter Server.

### Procedure

1. Verify that passwords are current and not set to expire soon.
2. Locate the `cleanup_orphaned_data_PostgresSQL.sql` script in the ISO image and copy it to your PostgreSQL server.
3. Log in to vCenter Server Appliance as root user.
4. Run the cleanup script.

   /opt/vmware/PostgreSQL/1.0/bin/psql -U postgres -d VCDB -f *path*cleanup_orphaned_data_Postgres.sql

   The cleanup script cleans and purges any unnecessary or orphaned data in your vCenter Server database that is not used by any vCenter Server component.
5. Make a full backup of the vCenter Server database and the vCenter Inventory Service database.

### Results

Your database is prepared for the vCenter Server upgrade.

## 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.

When upgrading a Microsoft SQL database, the permissions must be set correctly.

Table 3-1. 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.<br>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 3-1. 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 VIEW SERVER STATE TO [vpxuser] | Provides access to SQL Server DMV views and sp_lock execution. |
| GRANT VIEW ANY DEFINITION TO [vpxuser] | Necessary for providing the user with the privileges to see metadata for SQL Server objects. |

When upgrading an Oracle database, the permissions must be set correctly.

Table 3-2. 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.<br>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.<br>This permission is not required after deployment. |
| GRANT SELECT ON dba_lock TO VPXADMIN | Necessary for determining existing locks on the vCenter Server database. |

Table 3-2. Oracle Database Permissions for vCenter Server (continued)

| Permission | Description |
|---|---|
| GRANT SELECT ON dba_tablespaces TO VPXADMIN | Necessary during upgrade for determining the required disk space.<br>This permission is not required after deployment. |
| GRANT SELECT ON dba_temp_files TO VPXADMIN | Necessary during upgrade for determining the required disk space.<br>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_$session TO VPXADMIN | View used to determine existing locks on the vCenter Server database. |
| GRANT UNLIMITED TABLESPACE TO VPXADMIN | Necessary for granting unlimited tablespace permissions to the vCenter Server database user. |
| GRANT SELECT ON v_$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.

## 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.

**Results**

vCenter Server communication is confirmed. You can continue to prepare other components of your environment.

# Verify Network Prerequisites Before Upgrading

Verify that your network is set up correctly and meets connectivity prerequisites for upgrading vCenter Server.

For information on creating a PTR record, see the documentation for your vCenter Server host operating system.

For information about configuring Active Directory, see the Microsoft Web site.

Domain users that are part of a Windows Administrators group with vCenter Server Administrator permission cannot be used to authenticate vCenter Server during upgrade and do not have vCenter Server permission after upgrade.

**Procedure**

1. Verify that the fully qualified domain name (FQDN) of the system where you will upgrade vCenter Server is resolvable. To verify that the FQDN is resolvable, type **nslookup -nosearch -nodefname *your_vCenter_Server_fqdn*** at a command-line prompt.

   If the FQDN is resolvable, the **nslookup** command returns the IP and name of the domain controller machine.
2. Verify that DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server.

   When you upgrade vCenter Server, the installation of the web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server from its IP address.

   Reverse lookup is implemented by using PTR records.

3 If you use DHCP instead of a manually assigned (static) IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Test the update by pinging the computer name.

   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.

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

5 If you intend to use Active Directory as an identity source, verify that it is set up correctly. The DNS of the vCenter Single Sign-On Server host machine must contain both lookup and reverse lookup entries for the domain controller of the Active Directory.

   For example, pinging *mycompany.com* should return the domain controller IP address for *mycompany*. Similarly, the `ping -a` command for that IP address should return the domain controller host name.

   Avoid trying to correct name resolution issues by editing the hosts file. Instead, make sure that the DNS server is correctly set up.

6 Before the upgrade, select the domain user to use for upgrading vCenter Server. Give that domain user exclusive administrator permission for vCenter Server, not as part of a Windows Administrators group.

#### Results

Your network is ready for vCenter Server upgrade.

#### What to do next

Prepare other components of your environment.

## Verify Load Balancer Before Upgrading vCenter Server

If you are using a load balancer for high availability for vCenter Single Sign-On, you must verify that it is supported and configured correctly before upgrading to vCenter Server 6.0.

In environments with less than four vCenter Server systems, VMware typically recommends a single Platform Services Controller instance and the associated vCenter Single Sign-On service. In larger environments, consider using multiple Platform Services Controller instances, protected by a network load balancer. The white paper *vCenter Server 6.0 Deployment Guide* on the VMware website discusses this setup. For current information on maximums, see the *Configuration Maximums*.

See the VMware Knowledge Base article http://kb.vmware.com/kb/2112736 for a vCenter Single Sign-On and Platform Services Controller high availability compatibility matrix.

### Prerequisites

### Procedure

1. Review the *vCenter Server 6.0 Deployment Guide* documentation for load balancing information.
2. If your load balancer is not supported, replace it with a supported load balancer.
3. Verify that the load balancer is correctly configured based on recommendations in *vCenter Server 6.0 Deployment Guide*.

# Prepare ESXi Hosts for vCenter Server Upgrade

Before upgrading to vCenter Server 6.0, you must prepare your ESXi hosts.

### Prerequisites

- To upgrade vCenter Server, your ESXi hosts must be at version 5.x. If your ESXi hosts are at an earlier version than 5.0, upgrade them to 5.x. Read and follow all best practices when upgrading your hosts to ESXi 5.x.
- For vCenter Server Appliance upgrade to version 6.0, your target host must be running ESXi 5.1 or later.
- For vCenter Server Appliance upgrade to version 6.0, the source and target ESXi hosts must not be in lockdown or maintenance mode.

### Procedure

1. To keep your current SSL certificates, back up the SSL certificates that are on the vCenter Server system before you upgrade to vCenter Server 6.0.

   The default location of the SSL certificates is `%allusersprofile%\Application Data\VMware\VMware VirtualCenter`.
2. If you have Custom or Thumbprint certificates, see Host Upgrades and Certificates to determine your preparatory steps.
3. If you have vSphere HA clusters, SSL certificate checking must be enabled.

   If certificate checking is not enabled when you upgrade, vSphere HA fails to configure on the hosts.

   a. Select the vCenter Server instance in the inventory panel.

   b. Select the **Manage** tab and the **General** subtab.

   c. Verify that the **SSL settings** field is set to **vCenter Server requires verified host SSL certificates**.

Results

Your ESXi hosts are ready for vCenter Server upgrade.

## Host Upgrades and Certificates

If you upgrade an ESXi host to ESXi 6.0 or later, the upgrade process replaces self-signed certificates with VMCA-signed certificates. The process retains custom certificates even if those certificates are expired or invalid.

The recommended upgrade workflow depends on the current certificates.

### Host Provisioned with Thumbprint Certificates

If your host is currently using thumbprint certificates, it is automatically assigned VMCA certificates as part of the upgrade process.

**Note** You cannot provision legacy hosts with VMCA certificates. You must upgrade to ESXi 6.0 or later.

### Host Provisioned with Custom Certificates

If your host is provisioned with custom certificates, usually third-party CA-signed certificates, those certificates remain in place. Change the certificate mode to Custom to ensure that the certificates are not replaced accidentally.

**Note** If your environment is in VMCA mode, and you refresh the certificates from the vSphere Web Client, any existing certificates are replaced with certificates that are signed by VMCA.

Going forward, vCenter Server monitors the certificates and displays information, for example, about certificate expiration, in the vSphere Web Client.

If you decide not to upgrade your hosts to vSphere 6.0 or later, the hosts retain the certificates that they are currently using even if the host is managed by a vCenter Server system that uses VMCA certificates.

Hosts that are being provisioned by Auto Deploy are always assigned new certificates when they are first booted with ESXi 6.0 software. When you upgrade a host that is provisioned by Auto Deploy, the Auto Deploy server generates a certificate signing request (CSR) for the host and submits it to VMCA. VMCA stores the signed certificate for the host. When the Auto Deploy server provisions the host, it retrieves the certificate from VMCA and includes it as part of the provisioning process.

You can use Auto Deploy with custom certificates.

## Change the Certificate Mode

In most cases, using VMCA to provision the ESXi hosts in your environment is the best solution. If corporate policy requires that you use custom certificates with a different root CA, you can edit the vCenter Server advanced options so that the hosts are not automatically provisioned with VMCA

certificates when you refresh certificates. You are then responsible for the certificate management in your environment.

You can use the vCenter Server advanced settings to change to thumbprint mode or to custom CA mode. Use thumbprint mode only as a fallback option.

Procedure

1 Select the vCenter Server that manages the hosts and click **Settings**.

2 Click **Advanced Settings**, and click **Edit**.

3 In the Filter box, enter **`certmgmt`** to display only certificate management keys.

4 Change the value of vpxd.certmgmt.mode to **custom** if you intend to manage your own certificates, and to **thumbprint** if you temporarily want to use thumbprint mode, and click **OK**.

5 Restart the vCenter Server service.

# Verify Preparations Are Complete for Upgrading vCenter Server

Verify that all components of your environment are ready to upgrade vCenter Server.

Your pre-upgrade configuration of vCenter Server services impacts your post-upgrade deployment of vCenter Server services.

- If you have vCenter Server 5.0, you can choose to configure either an embedded or an external Platform Services Controller instance during the upgrade. See Upgrade vCenter Server 5.0.
- If you have vCenter Server 5.1 or 5.5, you do not have a choice of deployment options during upgrade. See Upgrade vCenter Server 5.1 for Windows or Upgrade vCenter Server 5.5 for Windows.
- If your vCenter Server 5.1 or 5.5 services are deployed on the same virtual machine or physical server, the installer upgrades them to vCenter Server 6.0 with an embedded Platform Services Controller instance.
- If your vCenter Single Sign-On 5.1 or 5.5 service is deployed on a different virtual machine or physical server than vCenter Server, the installer upgrades the deployment to vCenter Server 6.0 with an external Platform Services Controller instance. For information on the consolidation of distributed services during the upgrade, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0 and vCenter Server Example Upgrade Paths.

**Note** You cannot change deployment of vCenter Server services after the upgrade.

For information about upgrading services, see About the vCenter Server 6.0 for Windows Upgrade Process. For information about upgrading an externally deployed vCenter Single Sign-On server, see Upgrade vCenter Single Sign-On 5.5 for External Deployment.

For information on synchronizing clocks, see Synchronizing Clocks on the vSphere Network.

To download the installer, see Download the vCenter Server for Windows Installer

### Prerequisites

After you have verified basic compatibility and upgrade readiness for your database, network, local database communication, and ESXi hosts, you are ready to perform the final tasks to assure upgrade readiness of your environment.

### Procedure

1. Log in as a member of the Administrators group on the host machine, with a user name that does not contain non-ASCII characters.
2. Make sure that your pre-upgrade configuration is correct for the post-upgrade deployment you want to achieve.
   - For vCenter Server 5.1 or 5.5, to upgrade to an embedded Platform Services Controller deployment, make sure that your vCenter Server and vCenter Single Sign-On instances are deployed on a single virtual machine or physical host.
   - For vCenter Server 5.1 or 5.5, to upgrade to an external Platform Services Controller deployment, make sure that your vCenter Single Sign-On is deployed on a separate virtual machine or physical host from its associated vCenter Server.
   - For vCenter Server 5.0, to upgrade to an embedded Platform Services Controller deployment, no pre-upgrade steps are required.
   - For vCenter Server 5.0, to upgrade to an external Platform Services Controller deployment, you must configure an external Platform Services Controller instance before upgrading vCenter Server. The Platform Services Controller information is used during the upgrade to register the external Platform Services Controller with vCenter Server.
3. Verify that the required services have started.
   - The vCenter Single Sign-On instance to which you are registering vCenter Server
   - VMware Certificate Authority
   - VMware Directory Service
   - VMware Identity Manager Service
   - VMware KDC Service
   - tcruntime-C-ProgramData-VMware-cis-runtime-VMwareSTSService
4. Before you install or upgrade a vSphere product, synchronize the clocks of all machines on the vSphere network.

5 If you do not intend to use vCenter Server 6.0 in evaluation mode, make sure that you have valid license keys for all purchased functionality. License keys from previous versions of vSphere continue to support the previous versions, however they do not support vCenter Server 6.0.

   If you do not have the license key, you can install in evaluation mode and use the vSphere Web Client to enter the license key later.

6 Close all instances of the vSphere Web Client.

7 Make sure that no processes conflict.

8 Download the installer.

**Results**

Your environment is ready for the upgrade of your vCenter Server.

## Synchronizing Clocks on the vSphere Network

Make sure that all 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 http://kb.vmware.com/kb/1318.

### 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.

This task explains how to set up NTP from the vSphere Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

**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.

## Downtime During the vCenter Server Upgrade

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

Expect downtime for vCenter Server as follows:

- The upgrade requires vCenter Server to be out of production for a minimum of 40 to 50 minutes, and can take much longer depending on the size of the database. The database schema upgrade takes approximately 10 to 15 minutes of this time. This estimate does not include host reconnection time after the upgrade.
- For vCenter Server deployments with an embedded database, the upgrade can require extra time to migrate the data from the legacy vCenter Server database to the new database instance.
- If Microsoft .NET Framework is not installed on the machine, a restart is required before starting the vCenter Server installation.
- vSphere Distributed Resource Scheduler (DRS) does not work while the upgrade is in progress. vSphere HA does work during the upgrade.

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

## 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.

# Required Information for Upgrading vCenter Server for Windows

The vCenter Server upgrade wizard prompts you for the upgrade 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 information that you might need when upgrading vCenter Server for Windows in the future.

You will see the default values in the table below only if you left the default values when you installed the source vCenter Server instance.

**Table 3-3. Information Required for Upgrading vCenter Server for Windows.**

| Required Information | | Default Value | Your Entry |
|---|---|---|---|
| vCenter Single Sign-On administrator user name | | administrator@vsphere.local | You cannot change the default user name during upgrade. |
| vCenter Single Sign-On administrator password | | | |
| Enable or disable Use the same credentials for vCenter Server | | Enabled by default | |
| vCenter Server user name | | administrator@vsphere.local | |
| vCenter Server password | | | |
| Syslog Service Port | | 514 | |
| Syslog Service TLS Port | | 1514 | |
| Auto Deploy Management Port | | 6502 | |
| Auto Deploy Service Port | | 6501 | |
| ESXi Dump Collector Port | | 6500 | |
| Destination Directory<br>The folder paths cannot contain non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%). | Directory to install vCenter Server | `C:\Program Files\VMware` | |
| | Directory to store data for vCenter Server | `C:\ProgramData\VMware` | |
| | Directory to which to export your 5.x data | `C:\ProgramData\VMware\VMware\vCenterServer\export` | |
| Join or do not participate in the VMware Customer Experience Improvement Program (CEIP)<br>For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*. | | Join the CEIP | |

# Required Information for Upgrading the vCenter Server Appliance

The vCenter Server Appliance upgrade 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.

**Important** Upgrades from vCenter Server Appliance 5.1 Update 3 and later to vCenter Server Appliance 6.0 are supported. To upgrade vCenter Server Appliance 5.0, you must first upgrade the vCenter Server Appliance to version 5.1 Update 3 or 5.5 Update 2 and then upgrade to vCenter Server Appliance 6.0. For information about upgrading vCenter Server Appliance 5.0 to version 5.1 Update 3, see the *VMware vSphere 5.1 Documentation*. For information about upgrading vCenter Server Appliance 5.0 to version 5.5 Update 2, see the *VMware vSphere 5.5 Documentation*.

You can use this worksheet to record the information that you need for upgrading a vCenter Server Appliance version 5.1 Update 3 or 5.5.x.

**Table 3-4. Information Required for Upgrading vCenter Server Appliance 5.1.x or 5.5..x**

| Required Information | | Default Value | Your Entry |
|---|---|---|---|
| IP address or FQDN of the target ESXi host on which you upgrade the vCenter Server Appliance | | | |
| Credentials of a user who has administrative rights on the target ESXi host | Target ESXi host user name | | |
| | Target ESXi host password | | |
| vCenter Server Appliance 6.0 name | | | |
| Version of the vCenter Server Appliance to upgrade to vCenter Server Appliance 6.0 | | | |
| Data for the vCenter Server Appliance to upgrade | vCenter Server Appliance IP address or FQDN | | |
| | vCenter Single Sign-On administrator user name | If you upgrade from vCenter Server Appliance 5.5.x this is administrator@vsphere.local | |
| | Password of the vCenter Single Sign-On administrator | | |
| | vCenter Server HTTPS port number | | |
| | Password of the root user | | |
| | Temporary upgrade files path | `/tmp/vmware/cis-export-folder` | |

Table 3-4. Information Required for Upgrading vCenter Server Appliance 5.1.x or 5.5..x (continued)

| Required Information | | Default Value | Your Entry |
|---|---|---|---|
| | Migrate performance & other historical data | Disabled by default | |
| IP address or FQDN of the source ESXi host on which the vCenter Server Appliance that you want to upgrade resides | | | |
| Credentials of a user who has administrative rights on the source ESXi host | Source ESXi host user name | | |
| | Source ESXi host password | | |
| vCenter Single Sign-On settings<br>Required only if you are upgrading a vCenter Server Appliance version 5.1.x | vCenter Single Sign-On password | | |
| | vCenter Single Sign-On domain name | | |
| | vCenter Single Sign-On site name | | |
| vCenter Server Appliance size.<br>The options vary depending on the size of your vSphere environment.<br>■ Tiny (up to 20 hosts, 400 virtual machines)<br>■ Small (up to 150 hosts, 3,000 virtual machines)<br>■ Medium (up to 300 hosts, 6,000 virtual machines)<br>■ Large (up to 1,000 hosts, 10,000 virtual machines) | | Tiny (up to 20 hosts, 400 virtual machines) | |
| Name of the datastore on which the new version of the vCenter Server Appliance is deployed | | | |
| Enable or disable thin disk mode. | | Disabled by default | |
| Temporary network for communication between the vCenter Server Appliance to upgrade and the new vCenter Server Appliance | | | |
| IP address version | | IPv4 | |
| IP address allocation method | | DHCP | |
| Static assignment settings | Network address | | |
| | Subnet mask | | |
| | Network gateway | | |
| | Network DNS servers, separated with commas | | |

Table 3-4. Information Required for Upgrading vCenter Server Appliance 5.1.x or 5.5..x (continued)

| Required Information | Default Value | Your Entry |
|---|---|---|
| Enable or disable SSH | Disabled by default | |
| Join or do not participate in the VMware Customer Experience Improvement Program (CEIP).<br>For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.<br>Required only if you are upgrading a vCenter Server Appliance with embedded vCenter Single Sign-On | Join the CEIP | |

# Upgrading and Updating vCenter Server for Windows

4

The vCenter Server upgrade includes a database schema upgrade, migration of vCenter Single Sign-On to Platform Services Controller, and upgrade of the vCenter Server software.

This chapter includes the following topics:



## About the vCenter Server 6.0 for Windows Upgrade Process

Upgrade options for vCenter Server on Windows depend on your existing deployment and version.

The vCenter Server for Windows upgrade process includes:

1 Export of the vCenter Server 5.x configuration

2 Uninstallation of the vCenter Server 5.x configuration

3 Installation of vCenter Server 6.0

4 Migration and configuration of vCenter Server 5.x services and data to the vCenter Server 6.0 deployment

The upgrade outcome depends on your current deployment:

- When upgrading from a vCenter Server 5.0 deployment, you can configure either an embedded or an external Platform Services Controller instance during the upgrade.
- When upgrading from a vCenter Server version 5.1 or version 5.5 deployment with services deployed on a single virtual machine (VM) or physical server, the software upgrades the deployment to vCenter Server with an embedded Platform Services Controller.
- When upgrading from a vCenter Server version 5.1 or version 5.5 deployment with vCenter Single Sign-On deployed on a different VM or physical server than vCenter Server, the software upgrades the deployment to vCenter Server with an external Platform Services Controller.
- When upgrading multiple instances of vCenter Server, you must upgrade sequentially and upgrade order matters. See Mixed-Version Transitional Environments During vCenter Server Upgrades

Figure 4-1. vCenter Server 5.0 for Windows Upgrade Workflow

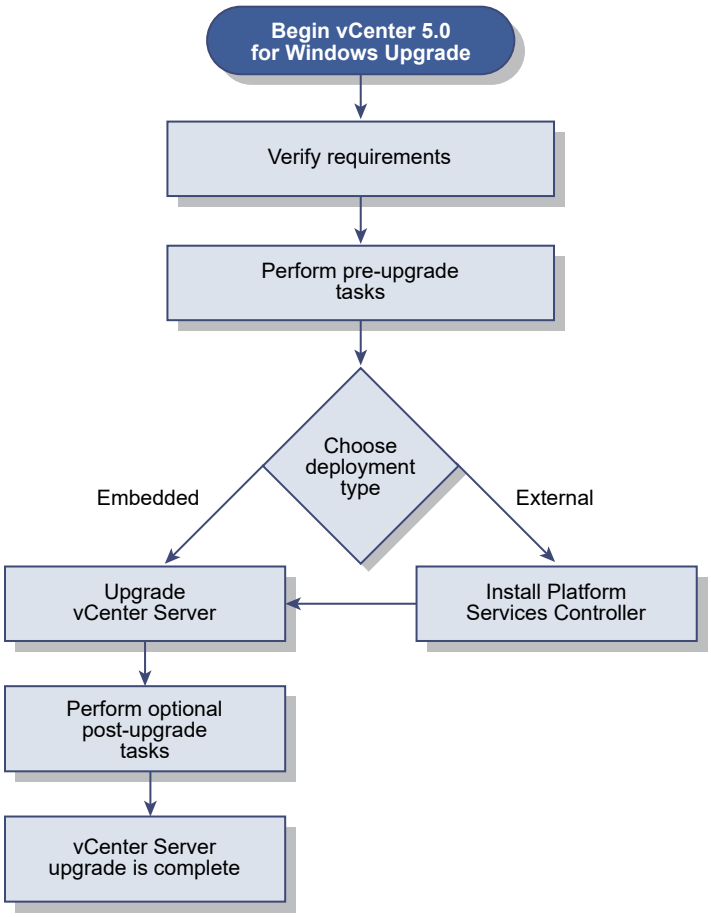
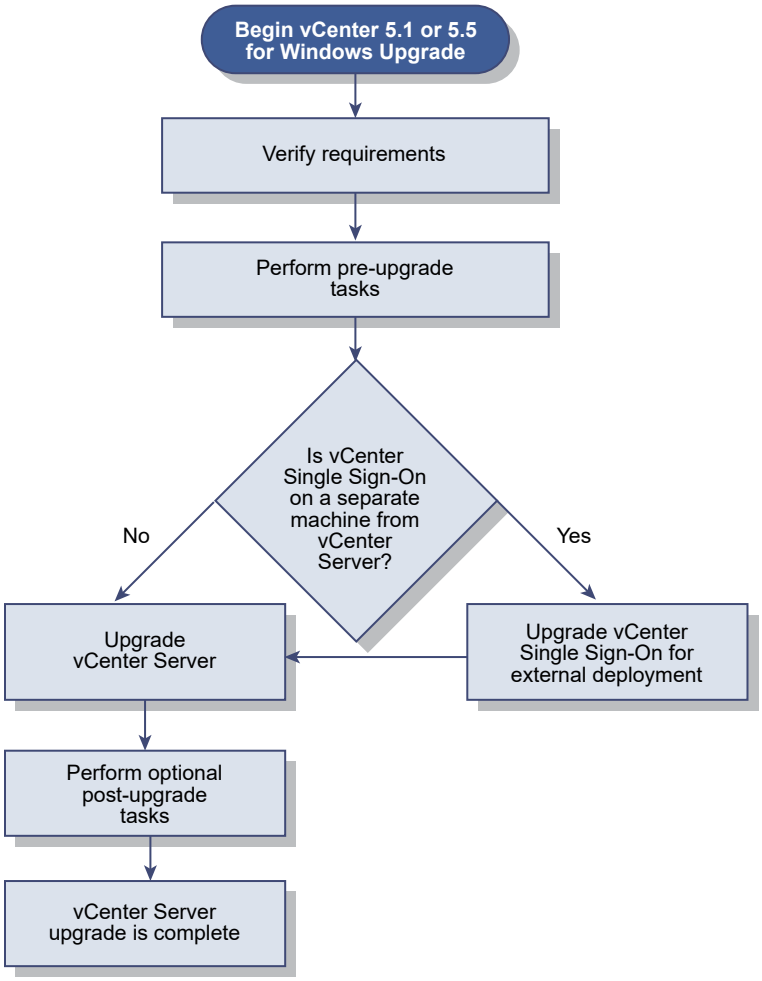


Figure 4-2. vCenter Server 5.1 or 5.5 for Windows Upgrade Workflow




You cannot uninstall or reinstall individual services during the upgrade process. For example, Inventory Service can no longer be deployed separately. It is part of the vCenter Server group of services for vCenter Server 6.0.

**Note** You cannot change the vCenter Server deployment model during upgrade. For example, you cannot change from vCenter Server with an embedded Platform Services Controller instance to vCenter Server with an external Platform Services Controller instance or the reverse.

## Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0

Custom installations of vCenter Server 5.1 or 5.5 for Windows that have services located across multiple machines are upgraded and migrated (if required) to the vCenter Server system during the upgrade process.

If all vCenter Server 5.x services are deployed in the same system, they are upgraded in place without any need for configuration after upgrade. However, if you have one or more services deployed remotely, the software migrates your service or services to the vCenter Server virtual machine or physical server during upgrade. Some services require reconfiguration or other actions after upgrade. vCenter Server 5.x for Windows services that are migrated to become part of the vCenter Server group of services during the upgrade process include:

- Inventory Services
- vSphere Web Client
- vSphere Auto Deploy
- vSphere Syslog Collector
- vSphere ESXi Dump Collector

vCenter Server and vCenter Single Sign-On are the only services that are not migrated. vCenter Single Sign-On instances are upgraded in place to become part of an external Platform Services Controller if they are deployed on a system other than the system where the vCenter Server resides.

Figure 4-3. Component Services Migrated to vCenter Server Group of Services

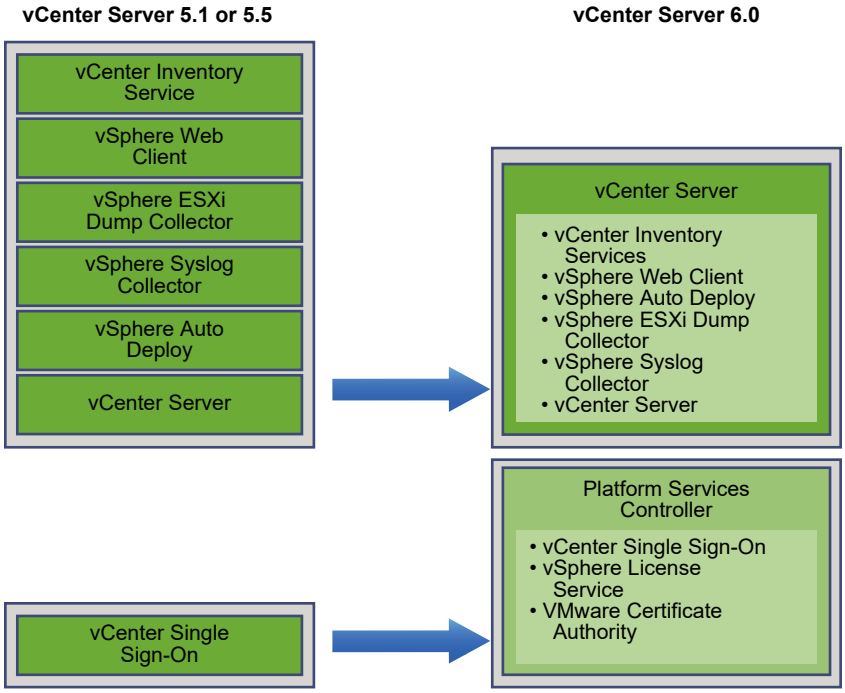


Table 4-1. vCenter Server 5.x Distributed Service Migration During Upgrade

| Service Name | Service Location Before Upgrade | Service Location After Upgrade | Post Upgrade Actions |
|---|---|---|---|
| vCenter Inventory Service | Not installed on the vCenter Server system | Installed on the vCenter Server system | vCenter Inventory Service 5.x data is copied to the Inventory Service 6.0 instance that is installed with vCenter Server 6.0. You do not need to copy it manually.<br>vCenter Inventory Service 5.x is still running but no longer used. It must be manually stopped and removed. |
| vSphere Web Client | Not installed on the vCenter Server system | Installed on the vCenter Server system | vCenter Server 5.x data is copied to the vSphere Web Client 6.0 instance that is installed with vCenter Server 6.0.<br>vSphere Web Client 5.x is still running but no longer used. It must be manually stopped and removed. |
| vSphere Auto Deploy | Not installed on the vCenter Server system | Migrated to vCenter Server system | vSphere Auto Deploy data is copied to the Auto Deploy 6.0 instance that is installed with vCenter Server 6.0.<br>Repoint vCenter Server DHCP settings to the migrated vSphere Auto Deploy service.<br>vCenter Server<br>vSphere Auto Deploy 5.x is still running but no longer used. It must be manually stopped and removed. |
| vSphere Syslog Collector | Not installed on the vCenter Server system | Installed on the vCenter Server system<br>Data is not migrated. Configurations for ports, protocols, and rotation log size are preserved. | ■ ESXi system information might remain on an old system until you relocate it.<br>■ ESXi hosts might require reconfiguration to point to the new vSphere Syslog Collector server. |
| vSphere ESXi Dump Collector | Not installed on the vCenter Server system | Installed on the vCenter Server system<br>Data is not migrated. | ■ ESXi core dump data might remain on an older system until you migrate it.<br>■ ESXi hosts might require reconfiguration to point to the new vSphere ESXI Dump server. |

For more information about upgrade scenarios, see vCenter Server Example Upgrade Paths. For information about service reconfigurations that are required after upgrade, see Reconfigure Migrated vCenter Server Services After Upgrade

# 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 Customer Connect 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.

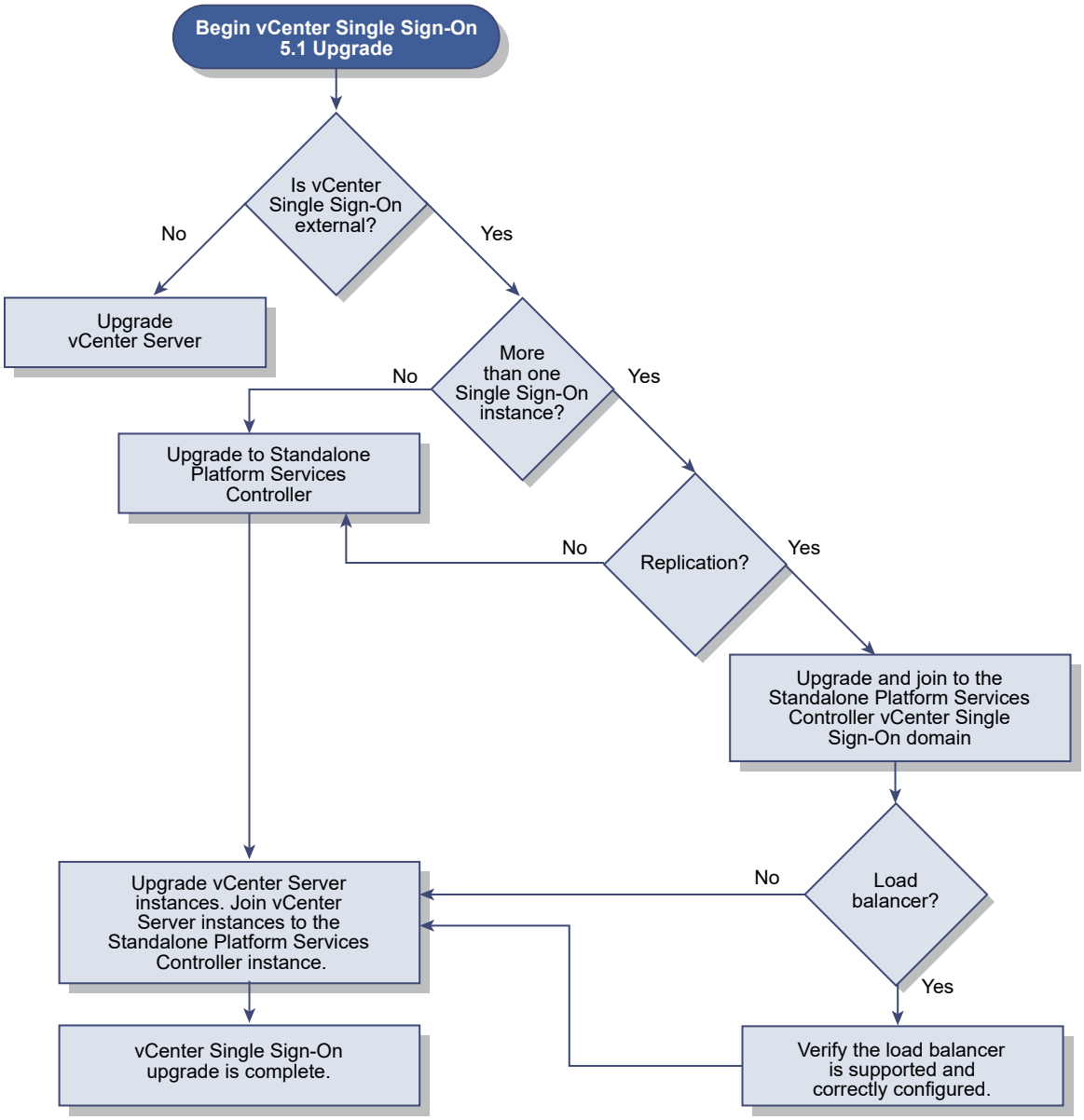
   See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

3. Mount the ISO image to the Windows virtual machine or physical server on which you want to install vCenter Server for Windows.

# Upgrade vCenter Single Sign-On 5.1 for External Deployment

You can upgrade your externally deployed vCenter Single Sign-On 5.1 to an externally deployed Platform Services Controller instance by using the vCenter Server for Windows installer.

Figure 4-4. vCenter Single Sign-On 5.1 Upgrade Workflow for Windows




If you are upgrading an externally deployed vCenter Single Sign-On 5.1 instance to an externally deployed Platform Services Controller instance in a mixed-version environment, any vCenter Server 5.1 instances continue to operate with the upgraded Platform Services Controller exactly as they did with the vCenter Single Sign-On without any problems or required actions.

- For more information about how vCenter Single Sign-On affects your upgrade, see How vCenter Single Sign-On Affects Upgrades.
- For information on vCenter Server behavior in mixed-version environments, see Mixed-Version Transitional Environments During vCenter Server Upgrades.
- For information on deployment options, see vCenter Server Deployment Models.

### Prerequisites

- Your current vCenter Single Sign-On must have been installed on a separate virtual machine or physical server from your vCenter Server instance.
- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See Chapter 3 Before Upgrading vCenter Server.
- Verify that you have made a backup of your vCenter Server configuration and database.
- Download the vCenter Server Installer. See Download the vCenter Server for Windows Installer.

**Note** A vCenter Single Sign-On 5.1 instance that is deployed on the same virtual machine or physical server as vCenter Server 5.1 is automatically upgraded to an embedded Platform Services Controller instance when you upgrade to vCenter Server 6.0.

### Procedure

1. Download the vCenter Server for Windows ISO file. Extract the ISO file locally, or mount the ISO file as a drive.
2. In the software installer, double-click the **`autorun.exe`** file to start the installer.
3. Select vCenter Server for Windows and click Install.

   The installer runs pre-upgrade checks in the background to discover your existing vCenter Single Sign-On settings and notify you of any problems that can affect your upgrade process. The vCenter Server installer opens to the Welcome page.
4. Verify the detected information and upgrade path.

   If you see a dialog box identifying missing requirements instead of a Welcome screen, follow the instructions in the dialog box.
5. Review the Welcome page and accept the license agreement.

   The installer runs pre-upgrade checks in the background to detect any issues that can cause the upgrade to fail. You might receive a warning if the old certificates do not meet current VMware security standards.
6. Upgrade vCenter Single Sign-On instances.

   You can create or join a Platform Services Controller site.

   - If this is the first or primary vCenter Single Sign-On instance, upgrade it to a new standalone Platform Services Controller instance by configuring a new vCenter Single Sign-On domain name and site name.
   - If you have two or more vCenter Single Sign-On instances and this is the second or an additional vCenter Single Sign-On instance, join it to the vCenter Single Sign-On site of the primary Platform Services Controller to enable replication.

Replication information is retained during the upgrade.

The vCenter Single Sign-On 5.1 domain '"System-Domain" is migrated to the new domain you choose.

7 Configure the ports and click Next.

The installer checks the availability of the selected ports and displays an error message if a selected port cannot be used.

8 Configure the install, data, and export directories and click Next.

The installer runs disk space and permission checks for the selected directories and displays an error message if the selected directories do not meet the requirements.

9 Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

10 Verify that the Summary page settings are correct. Verify that you have made a backup of your system and click Upgrade.

A progress indicator displays as the installer starts the upgrade process. When the process is complete, the installer verifies the upgrade.

11 Before clicking Finish, note the post-upgrade steps.

12 Click Finish to complete the upgrade.

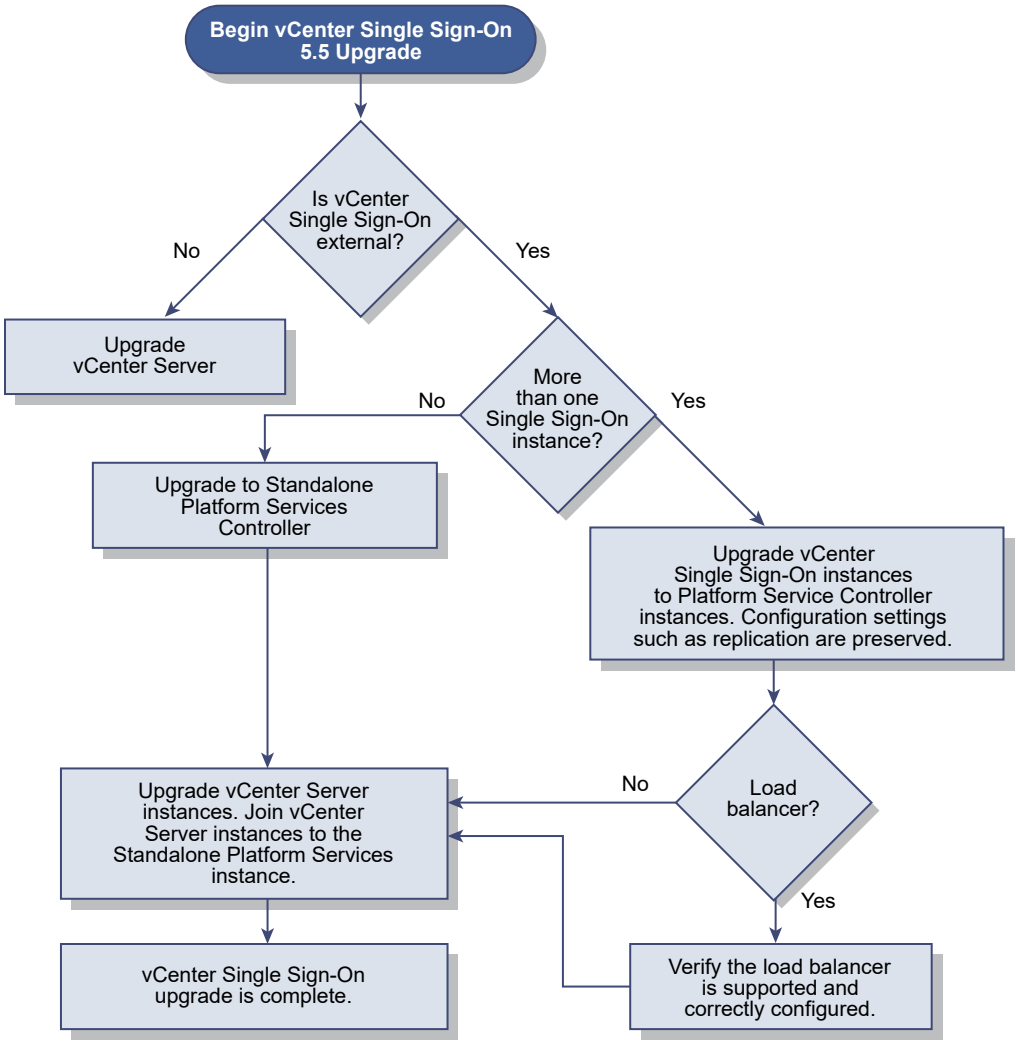
#### What to do next

After configuring an external Platform Services Controller instance, you are ready to upgrade your vCenter Server to an external deployment.

## Upgrade vCenter Single Sign-On 5.5 for External Deployment

You can upgrade your externally deployed vCenter Single Sign-On 5.5 to an externally deployed Platform Services Controller instance by using the vCenter Server for Windows installer.

Figure 4-5. vCenter Single Sign-On 5.5 Upgrade Workflow for Windows




If you are upgrading an externally deployed vCenter Single Sign-On 5.5 to an externally deployed Platform Services Controller in a mixed version environment, any vCenter Server 5.5 instances continue to operate with the upgraded Platform Services Controller exactly as they did with the vCenter Single Sign-On without any problems or required actions.

**Note** A vCenter Single Sign-On 5.5 deployed on the same VM or physical server as vCenter Server 5.5 is automatically upgraded to an embedded Platform Services Controller when you upgrade to vCenter Server 6.0.

- For more information about how vCenter Single Sign-On affects your upgrade, see How vCenter Single Sign-On Affects Upgrades.
- For information on vCenter Server behavior in mixed version environments, see Mixed-Version Transitional Environments During vCenter Server Upgrades.
- For information on deployment options, see vCenter Server Deployment Models.

### Prerequisites

- Your current vCenter Single Sign-On must have been installed on a separate virtual machine (VM) or physical server from your vCenter Server instance.
- Verify your configuration meets the upgrade requirements, see vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See Chapter 3 Before Upgrading vCenter Server
- Verify that you have made a backup of your vCenter Server configuration and database.
- To verify that the VMware Directory Service is in a stable state and can stop, manually restart it. The VMware Directory service must stopped for the vCenter Server upgrade software to uninstall vCenter Single Sign-On during the upgrade process.
- Download the vCenter Server Installer. See Download the vCenter Server for Windows Installer

### Procedure

1. Download the vCenter Server for Windows ISO file. Extract the ISO file locally, or mount the ISO file as a drive.
2. In the software installer, double-click the **`autorun.exe`** file to start the installer.
3. Select vCenter Server for Windows and click Install.

   The installer runs checks in the background to discover your existing vCenter Single Sign-On settings and notify you of any problems that can affect your upgrade process.

   The vCenter Server installer opens to the Welcome page.
4. Verify the detected information and upgrade path.

   If you see a dialog box identifying missing requirements instead of a Welcome screen, follow the instructions in the dialog box.
5. Review the Welcome page and accept the license agreement.
6. Enter the credentials for the **`administrator@vsphere.local`**.

   The installer runs pre-upgrade checks in the background to detect any issues that can cause the upgrade to fail. You might receive a warning if the old certificates do not meet current VMware security standards.
7. Follow the prompts to upgrade the vCenter Single Sign-On instance to a Platform Services Controller instance.

   You can create or join a Platform Services Controller instance.

   - If this is the first or primary vCenter Single Sign-On instance, upgrade it to a new standalone Platform Services Controller instance by configuring a new vCenter Single Sign-On domain name and site name.

- If you have two or more vCenter Single Sign-On instances and this is the second or an additional vCenter Single Sign-On instance, join it to the vCenter Single Sign-On site of the primary Platform Services Controller to enable replication.

Replication information is retained during the upgrade.

The vCenter Single Sign-On 5.5 domain *System-Domain* is migrated to the new domain you choose.

8 Configure the ports and click Next.

Verify 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.

The installer checks the availability of the selected ports and displays an error message if a selected port cannot be used.

9 Configure the install, data, and export directories and click Next.

The installer runs disk space and permission checks for the selected directories and displays an error message if the selected directories do not meet the requirements.

10 Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

11 Verify that the Summary page settings are correct. Verify that you have made a backup of your system and click Upgrade.

A progress indicator displays as the installer starts the upgrade process. When the process is complete, the installer verifies the upgrade.

12 Before clicking Finish, note the post upgrade steps.

13 Click Finish to complete the upgrade.

### What to do next

After configuring an external Platform Services Controller instance, you are ready to upgrade your vCenter Server to an external deployment.

# Upgrade vCenter Server 5.0

You can upgrade your existing vCenter Server 5.0 deployment by using the vCenter Server for Windows installer.

When you upgrade from vCenter Server 5.0, you can configure either an embedded or an external Platform Services Controller during the upgrade.

- Ports that are in use by vCenter Server are preserved. You cannot change ports during the upgrade. For information on required ports, see Required Ports for vCenter Server and Platform Services Controller.

- The installer automatically migrates the database from Microsoft SQL Server Express to the PostgreSQL (vPostgres) database that is included in vCenter Server. For information about migrating from Microsoft SQL Server Express to Microsoft SQL Server before upgrading to VC 6.0, see the VMware knowledge base article at http://kb.vmware.com/kb/1028601 and the Microsoft documentation. To upgrade without migrating to the PostgreSQL database, see the VMware knowledge base article http://kb.vmware.com/kb/2109321.
- For information on deployment options, see vCenter Server Deployment Models and About the vCenter Server 6.0 for Windows Upgrade Process.
- For information on post-upgrade steps, see Chapter 6 After Upgrading vCenter Server.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the upgrade preparation tasks. See Chapter 3 Before Upgrading vCenter Server
- Verify that you have made a backup of your vCenter Server configuration and database.
- Download the vCenter Server Installer. See Download the vCenter Server for Windows Installer

Procedure

1. Download the vCenter Server for Windows ISO file. Extract the ISO file locally, or mount the ISO file as a drive.
2. In the software installer, double-click the **`autorun.exe`** file to start the installer.
3. Select vCenter Server for Windows and click Install.

   The installer runs checks in the background to discover your existing settings and notify you of any problems that can affect your upgrade process.

   The vCenter Server installer opens to the Welcome page.
4. When the installer displays the detected information and the upgrade path, verify that it is correct.

   If you see a dialog box identifying missing requirements instead of a Welcome screen, follow the instructions in the dialog box.
5. Complete the installation wizard steps and accept the license agreement.
6. Enter your vCenter Server administrator credentials.

   The installer runs checks in the background to detect any issues that can cause the upgrade to fail. You might receive a warning if the old certificates do not meet current VMware security standards.

7 Select the vCenter Server deployment model.

- If you choose vCenter Server with an embedded Platform Services Controller, create or join a vCenter Single Sign-On domain and site and click Next.

  **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.

- If you choose vCenter Server with an external Platform Services Controller, enter the information for the external Platform Services Controller and click Next.

For an embedded Platform Services Controller instance, the installer migrates the vCenter Single Sign-On domain *System-Domain* to the new domain that is chosen for the Platform Services Controller. For an external Platform Services Controller, the installer validates the information that is entered by connecting to the Platform Services Controller instance using the credentials entered.

8 Configure the ports and click Next.

The installer checks for the availability of the selected ports and displays an error message if a selected port cannot be used.

9 Configure the install, data and export data directories and click Next.

The installer runs disk space and permission checks for the selected directories and displays an error message if the selected directories do not meet the requirements.

10 If you chose the embedded deployment, review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

11 Review the Summary page to verify that the settings are correct. Verify that you have made a backup of the vCenter Server machine and the vCenter Server database and click Upgrade.

A progress indicator displays as the installer starts the upgrade process. When the process is complete, the installer verifies the upgrade.

12 Before clicking Finish, note the post-upgrade steps.

13 Click Finish to complete the upgrade.

**Results**

Your vCenter Server for Windows upgrade is complete. For information on post-upgrade tasks, see Chapter 6 After Upgrading vCenter Server.

# Upgrade vCenter Server 5.1 for Windows

You can upgrade your existing vCenter Server 5.1 deployment by using the vCenter Server for Windows installer.

Your vCenter Server 5.1 configuration of services determines your post-upgrade deployment of components and services.

- If your vCenter Single Sign-On 5.1 is located on the same virtual machine or physical server as your vCenter Server, the installer upgrades your configuration to vCenter Server with an embedded Platform Services Controller deployment.
- If your vCenter Single Sign-On 5.1 is located on a different virtual machine or physical server than your vCenter Server, the installer upgrades your configuration to vCenter Server with an external Platform Services Controller deployment.
- vCenter Server 5.1 ports that are in use by vCenter Server and vCenter Single Sign-On are preserved. You cannot change ports during the upgrade. For information on required ports, see Required Ports for vCenter Server and Platform Services Controller.
- vCenter Server services are no longer deployed separately from vCenter Server. Separately deployed 5.1 services are upgraded and migrated to the vCenter Server virtual machine or physical server during the upgrade process. For details on service migration, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0 and vCenter Server Example Upgrade Paths.
- The installer automatically migrates the database from Microsoft SQL Server Express to the PostgreSQL database that is included in vCenter Server. For information about migrating from Microsoft SQL Server Express to Microsoft SQL Server before upgrading to VC 6.0, see the VMware knowledge base article at http://kb.vmware.com/kb/1028601 and the Microsoft documentation. To upgrade without migrating to the PostgreSQL database, see the VMware knowledge base article http://kb.vmware.com/kb/2109321.

**Note** If you are using an external vCenter Single Sign-On instance, you must upgrade it to Platform Services Controller 6.0 before upgrading your vCenter Server 5.5 instances to 6.0. See Upgrade vCenter Single Sign-On 5.1 for External Deployment.

- For information on deployment options, see vCenter Server Deployment Models and About the vCenter Server 6.0 for Windows Upgrade Process.
- For information on vCenter Server behavior in mixed version environments, see Mixed-Version Transitional Environments During vCenter Server Upgrades.
- For information about upgrading vCenter Single Sign-On 5.1, see Upgrade vCenter Single Sign-On 5.1 for External Deployment.
- For information on post-upgrade steps, see Chapter 6 After Upgrading vCenter Server.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See Chapter 3 Before Upgrading vCenter Server
- Verify that you have made a backup of your vCenter Server configuration and database.

- Download the vCenter Server Installer. See Download the vCenter Server for Windows Installer

Procedure

1 Download the vCenter Server for Windows ISO file. Extract the ISO file locally, or mount the ISO file as a drive.

2 In the software installer, double-click the **autorun.exe** file to start the installer.

3 Select vCenter Server for Windows and click Install.

The installer runs checks in the background to discover your existing vCenter Single Sign-On settings and notify you of any problems that can affect your upgrade process.

The vCenter Server installer opens to the Welcome page.

4 When the installer displays the detected information and upgrade path, verify that it is correct.

If you see a dialog box identifying missing requirements instead of a Welcome screen, follow the instructions in the dialog box.

5 Complete the installation wizard steps and accept the license agreement.

The installer runs pre-upgrade checks in the background to detect any issues that can cause the upgrade to fail. You might receive a warning if the old certificates do not meet current VMware security standards.

6 Configure the Platform Services Controller instance.

- If vCenter Server and vCenter Single Sign-On are installed in the same machine, configure Platform Services Controller and click Next.
- If vCenter Server and vCenter Single Sign-On are not located in the same machine, enter the prompted information for the external Platform Services Controller and click Next.

For an embedded Platform Services Controller, the installer migrates the vCenter Single Sign-On domain *System-Domain* to the new domain that is chosen the Platform Services Controller. For an external Platform Services Controller, the installer validates the information that is entered by connecting to the Platform Services Controller instance using the credentials entered.

7 Configure the ports and click Next.

The installer checks for the availability of the selected ports and displays an error message if a selected port cannot be used.

8 Configure the install, data, and export data directories and click Next.

The installer runs disk space and permission checks for the selected directories and displays an error message if the selected directories do not meet the requirements.

9 Review the Summary page to verify that the settings are correct. Verify that you have made a backup of the vCenter Server machine and the vCenter Server database and click Upgrade.

   A progress indicator displays as the installer starts the upgrade process. When the process is complete, the installer verifies the upgrade.

10 Before clicking Finish, note the post-upgrade steps.

11 Click Finish to complete the upgrade.

**Results**

Your vCenter Server for Windows upgrade is complete. For information on post-upgrade tasks, see Chapter 6 After Upgrading vCenter Server.

# Upgrade vCenter Server 5.5 for Windows

You can upgrade your existing vCenter Server 5.5 deployment by using the vCenter Server for Windows installer.

Your vCenter Server 5.5 configuration of services determines your post-upgrade deployment of components and services.

- If your vCenter Single Sign-On 5.5 is located on the same virtual machine or physical server as your vCenter Server, the installer upgrades your configuration to vCenter Server with an embedded Platform Services Controller deployment.
- If your vCenter Single Sign-On 5.5 is located on a different virtual machine or physical server than your vCenter Server: the installer upgrades your configuration to vCenter Server with an external Platform Services Controller deployment.
- vCenter Server 5.5 ports that are in use by vCenter Server and vCenter Single Sign-On are preserved. You cannot change ports during the upgrade. For information on required ports, see Required Ports for vCenter Server and Platform Services Controller.
- vCenter Server services are no longer deployed separately from vCenter Server. Separately deployed 5.5 services are upgraded and migrated to the vCenter Server virtual machine or physical server during the upgrade process. For details on service migration, see Migration of Distributed vCenter Server for Windows Services During Upgrade to vCenter Server 6.0 and vCenter Server Example Upgrade Paths.

- The installer automatically migrates the database from Microsoft SQL Server Express to the PostgreSQL database that is included in vCenter Server. For information about migrating from Microsoft SQL Server Express to Microsoft SQL Server before upgrading to VC 6.0, see the VMware knowledge base article at http://kb.vmware.com/kb/1028601 and the Microsoft documentation. To upgrade without migrating to the PostgreSQL database, see the VMware knowledge base article http://kb.vmware.com/kb/2109321.

**Note** If you are using an external vCenter Single Sign-On, you must upgrade it to Platform Services Controller 6.0 before upgrading your vCenter Server 5.5 instances to 6.0. See Upgrade vCenter Single Sign-On 5.5 for External Deployment.

- For information on deployment options, see vCenter Server Deployment Models and About the vCenter Server 6.0 for Windows Upgrade Process.
- For information on vCenter Server behavior in mixed version environments, see Mixed-Version Transitional Environments During vCenter Server Upgrades.
- For information about upgrading vCenter Single Sign-On 5.5, see Upgrade vCenter Single Sign-On 5.5 for External Deployment.
- For information on post-upgrade steps, see Chapter 6 After Upgrading vCenter Server.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See Chapter 3 Before Upgrading vCenter Server
- Verify that you have made a backup of your vCenter Server configuration and database.
- To verify that the VMware Directory Service is in a stable state and can stop, manually restart it. The VMware Directory service must stopped for the vCenter Server upgrade software to uninstall vCenter Single Sign-On during the upgrade process.
- Download the vCenter Server Installer. See Download the vCenter Server for Windows Installer.
- If your vCenter Single Sign-On 5.5 is located on a different virtual machine or physical server than your vCenter Server, make sure you upgrade vCenter Single Sign-On 5.5 before you start the upgrade of vCenter Server 5.5. See Upgrade vCenter Single Sign-On 5.5 for External Deployment

Procedure

1. Download the vCenter Server for Windows ISO file. Extract the ISO file locally, or mount the ISO file as a drive.
2. In the software installer, double-click the **`autorun.exe`** file to start the installer.

3 Select vCenter Server for Windows and click Install.

The installer runs checks in the background to discover your existing vCenter Single Sign-On settings and notify you of any problems that can affect your upgrade process.

The vCenter Server installer opens to the Welcome page.

4 Click **Next** and accept the license agreement.

5 Enter your vCenter Server and vCenter Single Sign-On credentials.

| Option | Action |
|---|---|
| If vCenter Single Sign-On is installed on the same virtual machine or physical server | 1 Enter your vCenter Single Sign-On credentials.<br>2 (Optional) Deselect the **Use the same credentials for vCenter Server** check box to use different credentials for the vCenter Server user, and provide the credentials that you want to use.<br>3 Click **Next**.<br>The installer runs checks in the background to detect any issues that can cause the upgrade to fail. You might receive a warning if the old certificates do not meet current VMware security standards. |
| If vCenter Single Sign-On is installed on a different virtual machine or physical server | 1 Enter your vCenter Server credentials, and click **Next**.<br>The installer runs checks in the background to detect any issues that can cause the upgrade to fail.<br>2 Register your vCenter Server with a vCenter Single Sign-On instance in an existing Platform Services Controller 6.0.<br>a (Optional) Change the default vCenter Single Sign-On HTTPS port.<br>b Enter your vCenter Single Sign-On administrator password, and click **Next**.<br>3 Verify the certificate provided by the remote server. |

6 Configure the ports and click Next.

Verify 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.

The installer checks for the availability of the selected ports, and displays an error message if a selected port cannot be used.

7 Configure install, data, and export data directories and click Next.

The installer runs disk space and permission checks for the selected directories, and displays an error message if the selected directories do not meet the requirements.

8 Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

9 Review the Summary page to verify that the settings are correct. Select the checkbox to verify that you have made a backup of the vCenter Server machine and the vCenter Server database and click Upgrade.

   The installer starts the upgrade process and displays a progress indicator. When the process is complete, the installer verifies the upgrade.

10 Before clicking Finish, take note of the post upgrade steps.

11 Click Finish to complete the upgrade.

### Results

Your vCenter Server for Windows upgrade is complete. For information on post-upgrade tasks, see Chapter 6 After Upgrading vCenter Server.

## Update the Java Components and vCenter Server tc Server with VIMPatch

You can separately update the Java version of all vCenter Server components depending on JRE server by using the `VIMPatch` ISO file.

You can apply the patch without reinstalling the vCenter Server components. The patch delivers updates for JRE.

### Prerequisites

- Download the Java Components patch from VMware downloads page at https://my.vmware.com/group/vmware/patch. The name format is `VMware-VIMPatch-6.0.0-`*`build_number`*`-`*`YYYYMMDD`*`.iso`.
- Stop any vCenter Server component operations, as when you apply the patch, all running services will be stopped.

### Procedure

1 Mount the `VMware-VIMPatch-6.0.0-`*`build_number`*`-`*`YYYYMMDD`*`.iso` to the system where the vCenter Server component is installed.

2 Double-click *`ISO_mount_directory`*`/autorun.exe`.

   A vCenter Server Java Components Update wizard opens.

3 Click **Patch All**.

   The patch checks whether the Java components are up to date and silently updates them if necessary.

# Upgrading and Patching the vCenter Server Appliance and Platform Services Controller Appliance

5

You can upgrade the vCenter Server Appliance by using the Client Integration Plug-In. You can update the vCenter Server Appliance and Platform Services Controller appliance with patches by using the Appliance Management Interface or by using the `software-packages` utility that is available in the appliance shell.

**Important** Upgrades from vCenter Server Appliance 5.1 Update 3 and later to vCenter Server Appliance 6.0 are supported. To upgrade a vCenter Server Appliance 5.0, you must first upgrade the vCenter Server Appliance to version 5.1 Update 3 or 5.5 Update 2 and then upgrade it to vCenter Server Appliance 6.0. For information about upgrading vCenter Server Appliance 5.0 to version 5.1 Update 3, see the *VMware vSphere 5.1 Documentation*. For information about upgrading vCenter Server Appliance 5.0 to version 5.5 Update 2, see the *VMware vSphere 5.5 Documentation*.

Version 6.0 of the vCenter Server Appliance uses the embedded PostgreSQL database, which is suitable for environments with up to 1,000 hosts and 10,000 virtual machines.

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.

For information about deploying the vCenter Server Appliance, see *vSphere Installation and Setup*.

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*.

This chapter includes the following topics:

# Upgrading the vCenter Server Appliance

To upgrade to the latest version of the vCenter Server Appliance, you must use the Client Integration Plug-In. All of the installation files necessary for the vCenter Server Appliance upgrade are included in an ISO file which you can download from the VMware Web site.

Before you upgrade the vCenter Server Appliance, download the ISO file and mount it to the Windows host machine from which you want to perform the upgrade. Install the Client Integration Plug-In, and then start the upgrade wizard.

For information about the vCenter Server Appliance upgrade requirements, see vCenter Server Appliance Requirements.

For information about the inputs that are required during the upgrade of the vCenter Server Appliance, see Required Information for Upgrading the vCenter Server Appliance.

The upgrade of the vCenter Server Appliance is a migration of the old version to the latest version, which results in deploying a new vCenter Server Appliance 6.0 on an ESXi host 5.0 or later. The configuration settings of the vCenter Server Appliance that you are upgrading are migrated and applied to the newly deployed vCenter Server Appliance. The new appliance is assigned a temporary IP address to facilitate the upgrade from the old appliance. The IP address and host name of the vCenter Server Appliance that you are upgrading are applied to the vCenter Server Appliance 6.0 as part of the upgrade process. At the end of the upgrade, the vCenter Server Appliance that you upgraded is powered off.

**Important** If the vCenter Server Appliance that you are upgrading is configured in a mixed IPv4 and IPv6 environment, only the IPv4 settings are preserved.

If the vCenter Server Appliance that you are upgrading uses a non-ephemeral distributed virtual port group, the port group is not preserved. After the upgrade, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group of the old appliance.

In a DHCP environment, the vCenter Server Appliance upgrade fails if the vCenter Server Appliance you are attempting to upgrade and the vCenter Server Appliance 6.0 run on hosts that are in different networks.

## About the vCenter Server Appliance Upgrade Process

You can upgrade from vCenter Server Appliance 5.1 Update 3 and 5.5.x to 6.0.

The upgrade process includes:

1 Exporting the vCenter Server Appliance 5.1 Update 3 or 5.5.x configuration.

2 Deploying the vCenter Server Appliance 6.0.

3 Migrating the vCenter Server Appliance 5.1 Update 3 or 5.5.x services and configuration data to the new vCenter Server Appliance 6.0 deployment.

   Non-ephemeral distributed virtual port groups are not migrated. After the upgrade, you can manually connect the new appliance to a non-ephemeral distributed virtual port group.

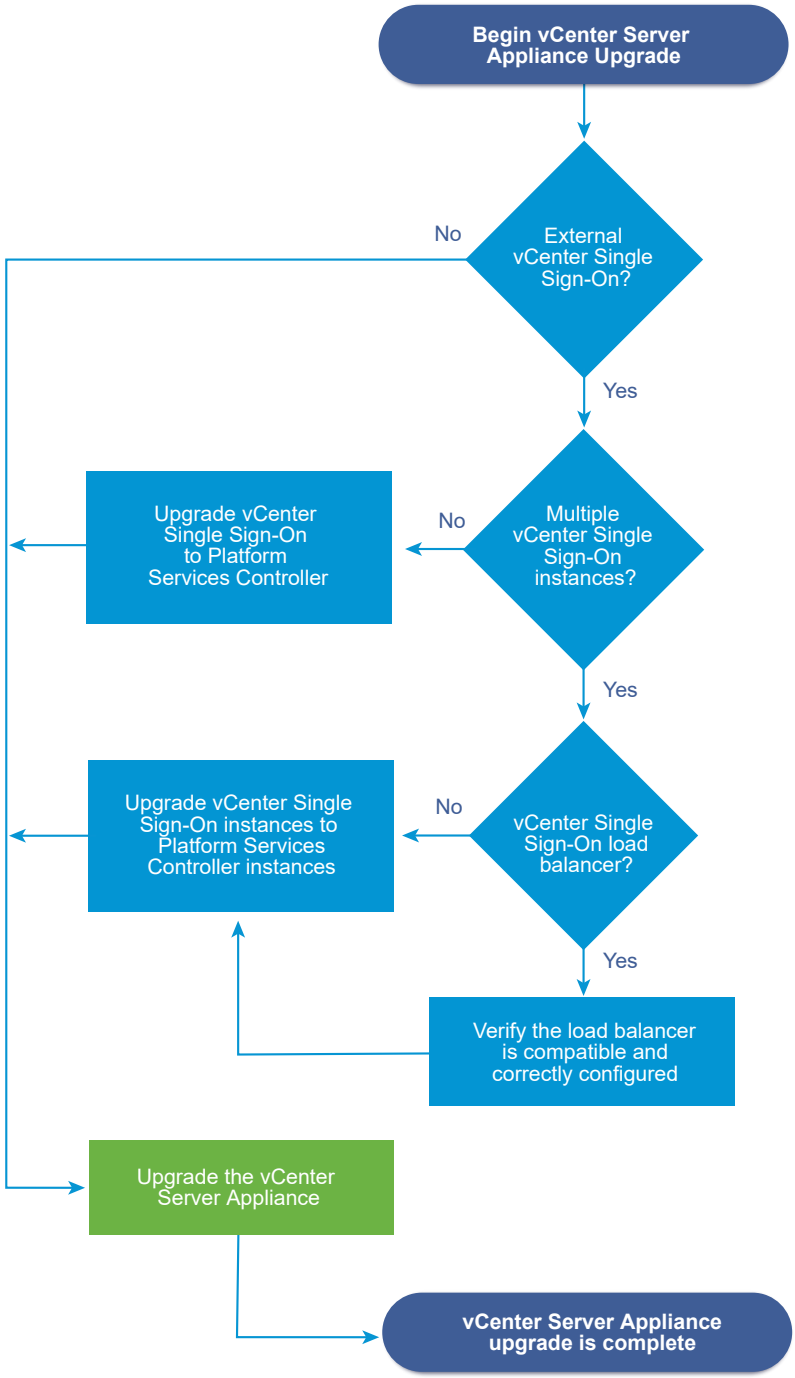
4 Powering off the vCenter Server Appliance 5.1 Update 3 or 5.5.x machine that you want to upgrade.

**Note** Upgrade of vCenter Server Appliance that is registered with an external vCenter Single Sign-On server is supported only for vCenter Server Appliance 5.5.x.

If your current vCenter Server Appliance version is earlier than 5.1 Update 3, you must upgrade to 5.1 Update 3 or later before upgrading to vCenter Server Appliance 6.0.

If you have multiple instances of vCenter Server Appliance, concurrent upgrades are not supported. You must upgrade one instance at a time.

Figure 5-1. vCenter Server Appliance Upgrade Workflow




- For vCenter Single Sign-On and Platform Services Controller compatibility information for the use of qualified load balancers and their requirements, see vCenter Single Sign-On and Platform Services Controller High Availability Compatibility Matrix.
- For the vCenter Server Appliance requirements, see vCenter Server Appliance Requirements.
- For vCenter Server Appliance upgrade preparation, see Chapter 3 Before Upgrading vCenter Server.

- For vCenter Server Appliance upgrade procedures, see Chapter 5 Upgrading and Patching the vCenter Server Appliance and Platform Services Controller Appliance.
- For vCenter Server Appliance post-upgrade procedures, see Chapter 6 After Upgrading vCenter Server.

## Download the vCenter Server Appliance Installer

Download the `.iso` installer for the vCenter Server Appliance and Client Integration Plug-in.

### Prerequisites

Create a Customer Connect 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

Download the vCenter Server Appliance Installer.

### Procedure

1. In the vCenter Server Appliance installer, 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**.

## Upgrade the vCenter Server Appliance with Embedded vCenter Single Sign-On

You can use the Client Integration Plug-In to upgrade a vCenter Server Appliance 5.1 Update 3 and 5.5.x that uses the embedded vCenter Single Sign-On instance to a vCenter Server Appliance 6.0 with an embedded Platform Services Controller.

You can deploy version 6.0 of vCenter Server Appliance only on hosts that are running ESXi 5.0 or later. Therefore, if the vCenter Server Appliance you want to upgrade is running on a host with a version earlier than ESXi 5.0, you must first install ESXi 5.0 or later, so that the upgrade wizard can migrate the 6.0 version of vCenter Server Appliance to that host.

To ensure that a vCenter Server Appliance instance has certificates with the correct FQDN, you must deploy it using one of the following methods:

- Start the vCenter Server Appliance using DHCP and the DHCP assigns a Fully Qualified Hostname.
- Deploy the vCenter Server Appliance to an existing vCenter Server and the OVF Properties for Hostname are set during deployment.

If you do not deploy vCenter Server Appliance with the correct FQDNs, you must regenerate the certificates. See VMware Component Manager Error During Startup After vCenter Server Appliance Upgrade.

### Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.
- Verify that the target ESXi host on which you deploy the vCenter Server Appliance is not in lockdown or maintenance mode.
- Verify that you have sufficient free disk space on the vCenter Server Appliance that you want to upgrade to accommodate the data for the upgrade.
- Verify that port 22 is open on the vCenter Server Appliance that you want to upgrade. The upgrade process establishes an inbound SSH connection to download the exported data from existing appliance.
- Verify that port 443 is open on the source ESXi host on which the vCenter Server Appliance that you want to upgrade resides. The upgrade process establishes an HTTPS connection to the source ESXi host to verify that the vCenter Server Appliance is ready for upgrade and to set up an SSH connection between the new and the existing appliance.
- Verify that the vCenter Server SSL certificate for your existing vCenter Server Appliance is configured correctly. See VMware Knowledge Base article 2057223.
- If you use an external database, back up the vCenter Server Appliance database.
- Create a snapshot of the vCenter Server Appliance that you want to upgrade.

- Install the new version of the Client Integration Plug-In. See Install the Client Integration Plug-In.

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 **Upgrade**.

4 In the Supported Upgrade warning message, click **OK** to start the vCenter Server Appliance upgrade wizard.

5 Read and accept the license agreement, and click **Next**.

6 Connect to the target server on which you want to deploy the vCenter Server Appliance, and click **Next**.

   a Enter the FQDN or IP address of the ESXi host.

   b Enter the user name and password of a user who has administrative privileges on the ESXi host, for example, the root user.

7 (Optional) Accept the certificate warning, if any, by clicking **Yes**.

8 Enter a name for the vCenter Server Appliance 6.0.

9 (Optional) Select the **Enable SSH** check box to enable SSH connection to the vCenter Server Appliance.

10 On the Connect to source appliance page enter the details of the appliance that you want to upgrade.

   a From the **Existing Appliance Version** drop-down menu, select the version of the vCenter Server Appliance that you want to upgrade to vCenter Server Appliance 6.0.

| Option | Description |
|---|---|
| **vCSA 5.1 U3** | Lets you upgrade a vCenter Server Appliance version 5.1 Update 3. |
| **vCSA 5.5** | Lets you upgrade a vCenter Server Appliance version 5.5.x. |

   b From the **Existing Appliance Type** drop-down menu, select **Embedded Platform Services Controller**.

c Under vCenter Server Appliance, enter the required data of the vCenter Server Appliance that you want to upgrade.

| Option | Action |
|---|---|
| **vCenter Server IP Address/FQDN** | Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade. |
| **vCenter Administrator User Name** | Enter the vCenter Single Sign-On administrator user name.<br>If you are upgrading vCenter Server Appliance 5.5.x, this is administrator@vsphere.local. |
| **vCenter Administrator Password** | Enter the password of the vCenter Single Sign-On administrator. |
| **vCenter HTTPS Port** | Optionally, change the default vCenter HTTPS port number.<br>The default value is 443. |
| **Appliance (OS) Root password** | Enter the password for the root user. |
| **Temporary Upgrade Files Path** | Optionally, change the default path to the folder in which to store the configuration data.<br>By default, all the data and information about the settings of the vCenter Server Appliance that you want to upgrade is exported to `/tmp/vmware/cis-export-folder`. The data is later migrated to the vCenter Server Appliance 6.0. |
| **Migrate Performance & other historical data** | Optionally, select whether you want to enable migration of optional performance and historical data stored in the database.<br>This includes information about alarms, events, statistics, and so on. If the information is large, the migration might slow down the upgrade. |

d Under Source ESXi Host, enter the information about the host on which the vCenter Server Appliance that you want to upgrade resides.

| Option | Description |
|---|---|
| **ESXi host IP address/FQDN** | IP address or FQDN of the ESXi host on which the vCenter Server Appliance that you want to upgrade resides. |
| **ESXi host user name** | User name of the user who has administrative rights on the primary host. |
| **ESXi host password** | Password of the administrator user. |

11 (Optional) Accept the warning message, if any, by clicking **Yes**.

12 Set up the vCenter Single Sign-On settings for the newly deployed appliance and click **Next**.

**Important** This step is mandatory only when you upgrade vCenter Server Appliance 5.1 Update 3. For upgrades from vCenter Server Appliance 5.5.x the vCenter Single Sign-On data is automatically migrated to the vCenter Server Appliance 6.0.

| Option | Description |
|---|---|
| **vCenter SSO Password** | Enter the password for vCenter Single Sign-On.<br>The password must be between 8 and 20 characters, and must contain at least one uppercase letter, one lowercase letter, one number, and one special character, such as, for example, a dollar sign ($), exclamation mark (!), brackets (()) or at sign (@). |
| **Confirm password** | Confirm the vCenter Single Sign-On password. |
| **SSO Domain name** | Enter the vCenter Single Sign-On domain name.<br>The domain name must comply with the RFC 1035 standards. |
| **SSO Site name** | Enter the vCenter Single Sign-On site name. |

13 On the Select appliance size page of the wizard, select the vCenter Server Appliance size for 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. |

14 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**.

15 Select the temporary network for communication between the vCenter Server Appliance that you want to upgrade and the newly deployed vCenter Server Appliance, select the vCenter Server Appliance IP allocation method, and click **Next**.

The networks displayed in the **Choose a temporary network** 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.

| Option | Description |
|---|---|
| **DHCP** | A DHCP server is used to allocate the IP address. |
| **Static** | You are prompted to enter the IP address and network settings.<br>a Enter a temporary IP address for the new vCenter Server Appliance.<br>b Enter the subnet mask.<br>c Enter the network gateway.<br>d Enter FQDNs or IP addresses of network DNS servers.<br>The names must be separated by commas. |

16 Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

17 On the Ready to complete page, review the settings for the vCenter Server Appliance upgrade and click **Finish** to complete the process.

18 (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.

19 Click **Close** to exit the wizard.

### Results

The vCenter Server Appliance is upgraded. The old vCenter Server Appliance is powered off and the new appliance starts.

### What to do next

If the old vCenter Server Appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.

# Upgrade the vCenter Server Appliance with External vCenter Single Sign-On

To upgrade a vCenter Server Appliance 5.5.x that is registered with an external vCenter Single Sign-On instance to a vCenter Server Appliance 6.0 with an external Platform Services Controller, you can use the Client Integration Plug-In.

You can deploy version 6.0 of vCenter Server Appliance only on hosts that are running ESXi 5.0 or later. Therefore, if the vCenter Server Appliance you want to upgrade is running on a host with a version earlier than ESXi 5.0, you must first install ESXi 5.0 or later, so that the upgrade wizard can migrate the 6.0 version of vCenter Server Appliance to that host.

Mixed-version environments are not supported for production and might result in limited functions of the environment. They are recommended only during the period when an environment is in transition between vCenter Server Appliance versions. After you upgrade all vCenter Server Appliance instances and join them to the Platform Services Controller, the Linked Mode function is replaced by Enhanced Linked Mode function.

To ensure that a vCenter Server Appliance instance has certificates with the correct FQDN, you must deploy it using one of the following methods:

- Start the vCenter Server Appliance using DHCP and the DHCP assigns a Fully Qualified Hostname.
- Deploy the vCenter Server Appliance to an existing vCenter Server and the OVF Properties for Hostname are set during deployment.

If you do not deploy vCenter Server Appliance with the correct FQDNs, you must regenerate the certificates. See VMware Component Manager Error During Startup After vCenter Server Appliance Upgrade.

### Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.
- Verify that the target ESXi host on which you deploy the vCenter Server Appliance is not in lockdown or maintenance mode.
- Verify that you have sufficient free disk space on the vCenter Server Appliance that you want to upgrade to accommodate the data for the upgrade.
- Verify that port 22 is open on the vCenter Server Appliance that you want to upgrade. The upgrade process establishes an inbound SSH connection to download the exported data from existing appliance.
- Verify that port 443 is open on the source ESXi host on which the vCenter Server Appliance that you want to upgrade resides. The upgrade process establishes an HTTPS connection to the source ESXi host to verify that the vCenter Server Appliance is ready for upgrade and to set up an SSH connection between the new and the existing appliance.

- Verify that the vCenter Server SSL certificate for your existing vCenter Server Appliance is configured correctly. See VMware Knowledge Base article 2057223.
- If you use an external database, back up the vCenter Server Appliance database.
- Upgrade your externally deployed vCenter Single Sign-On 5.5 to an externally deployed Platform Services Controller. For information about the upgrade of vCenter Single Sign-On 5.5, see Upgrade vCenter Single Sign-On 5.5 for External Deployment.
- Create a snapshot of the vCenter Server Appliance that you want to upgrade.
- Install the new version of the Client Integration Plug-In. See Install the Client Integration Plug-In.

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 **Upgrade**.
4. In the Supported Upgrade warning message, click **OK** to start the vCenter Server Appliance upgrade wizard.
5. Read and accept the license agreement, and click **Next**.
6. Connect to the target server on which you want to deploy the vCenter Server Appliance, and click **Next**.
   a. Enter the FQDN or IP address of the ESXi host.
   b. Enter the user name and password of a user who has administrative privileges on the ESXi host, for example, the root user.
7. (Optional) Accept the certificate warning, if any, by clicking **Yes**.
8. Enter a name for the vCenter Server Appliance 6.0.
9. (Optional) Select the **Enable SSH** check box to enable SSH connection to the vCenter Server Appliance.
10. On the Connect to source appliance page, enter the details of the appliance that you want to upgrade.
    a. From the **Existing Appliance Version** drop-down menu, select the version of the vCenter Server Appliance that you want to upgrade to vCenter Server Appliance 6.0.

| Option | Description |
|---|---|
| **vCSA 5.1 U3** | Lets you upgrade a vCenter Server Appliance version 5.1 Update 3. |
| **vCSA 5.5** | Lets you upgrade a vCenter Server Appliance version 5.5.x. |

    b. From the **Existing Appliance Type** drop-down menu, select **vCenter Server**.

c Under vCenter Server Appliance, enter the required data of the vCenter Server Appliance that you want to upgrade.

| Option | Action |
|---|---|
| **vCenter Server IP Address/FQDN** | Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade. |
| **vCenter Administrator User Name** | Enter the vCenter Single Sign-On administrator user name.<br>If you are upgrading vCenter Server Appliance 5.5.x, this is administrator@vsphere.local. |
| **vCenter Administrator Password** | Enter the password of the vCenter Single Sign-On administrator. |
| **vCenter HTTPS Port** | Optionally, change the default vCenter HTTPS port number.<br>The default value is 443. |
| **Appliance (OS) Root password** | Enter the password for the root user. |
| **Temporary Upgrade Files Path** | Optionally, change the default path to the folder in which to store the configuration data.<br>By default, all the data and information about the settings of the vCenter Server Appliance that you want to upgrade is exported to `/tmp/vmware/cis-export-folder`. The data is later migrated to the vCenter Server Appliance 6.0. |
| **Migrate Performance & other historical data** | Optionally, select whether you want to enable migration of optional performance and historical data stored in the database.<br>This includes information about alarms, events, statistics, and so on. If the information is large, the migration might slow down the upgrade. |

d Under Source ESXi Host, enter the information about the host on which the vCenter Server Appliance that you want to upgrade resides.

| Option | Description |
|---|---|
| **ESXi host IP address/FQDN** | IP address or FQDN of the ESXi host on which the vCenter Server Appliance that you want to upgrade resides. |
| **ESXi host user name** | User name of the user who has administrative rights on the primary host. |
| **ESXi host password** | Password of the administrator user. |

11 (Optional) Accept the warning message, if any, by clicking **Yes**.

12 On the Select appliance size page of the wizard, select the vCenter Server Appliance size for 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. |

| Option | Description |
|---|---|
| **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. |

13 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**.

14 Select the temporary network for communication between the vCenter Server Appliance that you want to upgrade and the newly deployed vCenter Server Appliance, select the vCenter Server Appliance IP allocation method, and click **Next**.

The networks displayed in the **Choose a temporary network** 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.

| Option | Description |
|---|---|
| **DHCP** | A DHCP server is used to allocate the IP address. |
| **Static** | You are prompted to enter the IP address and network settings.<br>a Enter a temporary IP address for the new vCenter Server Appliance.<br>b Enter the subnet mask.<br>c Enter the network gateway.<br>d Enter FQDNs or IP addresses of network DNS servers.<br>The names must be separated by commas. |

15 On the Ready to complete page, review the settings for the vCenter Server Appliance upgrade and click **Finish** to complete the 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.

### Results

The vCenter Server Appliance is upgraded. The old vCenter Server Appliance is powered off and the new appliance starts.

### What to do next

If the old vCenter Server Appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.

# Patching the vCenter Server Appliance and Platform Services Controller Appliance

VMware regularly releases patches for the vCenter Server Appliance that might be related to third-party products in the platform, core product functionality, or both. You can use the Appliance Management Interface or the appliance shell to apply patches to a vCenter Server Appliance that contains a vCenter Server with an embedded Platform Services Controller, a vCenter Server with an external Platform Services Controller, or a Platform Services Controller.

VMware distributes the available patches in two forms, one for ISO-based and one for URL-based models of patching.

- You can download the patch ISO images from https://my.vmware.com/group/vmware/patch.

  VMware publishes two types of ISO images that contain patches.

  | Download Filename | Description |
  |---|---|
  | `VMware-vCenter-Server-Appliance-`*`product_version-build_number`*`-patch-TP.iso` | Third-party patch for the vCenter Server Appliance and Platform Services Controller appliance, which contains only the fixes related to security and third-party products (e.g. JRE, tcServer, and SLES OS components). |
  | `VMware-vCenter-Server-Appliance-`*`product_version-build_number`*`-patch-FP.iso` | Full product patch for the vCenter Server Appliance and Platform Services Controller appliance, which contains the VMware software patches and the fixes related to security and third-party products (e.g. JRE, tcServer, and SLES OS components). |

- You can configure the vCenter Server Appliance and Platform Services Controller appliance to use a repository URL as a source of available patches. The appliance is preset with a default VMware repository URL.

  You can download the patches in ZIP format from the VMware Web site at https://my.vmware.com/web/vmware/downloads and build a custom repository on a local Web server. The download filename is `VMware-vCenter-Server-Appliance-`*`product_version-build_number`*`-updaterepo.zip`.

When there are available patches, you can select to apply only the third-party patches that are related to security and third-party products (e.g. JRE, tcServer, and SLES OS components), or you can apply all VMware software patches together with the third-party patches.

**Important** Third-party patches usually belong to the security category. You must always apply at least the patches related to security.

Before you update a vCenter Server Appliance with an external Platform Services Controller, you must apply the patches to the Platform Services Controller and its replicating partners, if any in the vCenter Single Sign-On domain. For more information, see Update sequence for vSphere 6.0 and its compatible VMware products.

# Patching the vCenter Server Appliance by Using the Appliance Management Interface

You can log in to the Appliance Management Interface of a vCenter Server Appliance that contains a vCenter Server with an embedded Platform Services Controller, a vCenter Server with an external Platform Services Controller, or a Platform Services Controller to view the installed patches, check for new patches and install them, and configure automatic checks for available patches.

To perform ISO-based patching, you download an ISO image, attach the ISO image to the CD/DVD drive of the appliance, check for available patches in the ISO image, and install the patches.

To perform URL-based patching, you check for available patches in a repository URL and install the patches. The vCenter Server Appliance is preset with a default VMware repository URL for the build profile of the appliance. You can configure the appliance to use the default VMware repository URL or a custom repository URL, for example, a repository URL that you previously built on a local Web server running within your data center.

## Log In to the vCenter Server Appliance Management Interface

Log in to the vCenter Server Appliance Management Interface to access the vCenter Server Appliance configuration settings.

**Note** The login session expires if you leave the vCenter Server Appliance Management Interface idle for 10 minutes.

### Prerequisites

Verify that the vCenter Server Appliance is successfully deployed and running.

### Procedure

1. In a Web browser, go to the vCenter Server Appliance Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
2. Log in as root.

   The default root password is the password you set while deploying the vCenter Server Appliance.

## Configure the Repository for URL-Based Patching

For URL-based patching, by default the vCenter Server Appliance is configured to use the default VMware repository URL that is preset for the build profile of the appliance. You can configure a custom repository URL as the current source of patches for your environment's requirements.

By default the current repository for URL-based patching is the default VMware repository URL.

**Note** You can use the `proxy.set` command to configure a proxy server for the connection between the vCenter Server Applianceand the repository URL. For more information about the API commands in the appliance shell, see *vCenter Server Appliance Configuration*.

If the vCenter Server Appliance is not connected to the Internet or if your security policy requires it, you can build and configure a custom repository that runs on a local Web server within your data center and replicates the data from the default VMware repository URL. Optionally, you can set up authentication policy for accessing the Web server that hosts the custom patching repository.

### Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

### Procedure

1 If you want to configure a custom repository URL, build the repository on your local Web server.

   a Download the vCenter Server Appliance patch ZIP file from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

   b On your Web server, create a repository directory under the root.

   For example, create the **`vc_update_repo`** directory.

   c Extract the ZIP file into the repository directory.

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

2 In the vCenter Server Appliance Management Interface, click **Update**.

3 Click **Settings**.

4 Select the Repository settings.

| Option | Description |
|---|---|
| **Use default repository** | Uses the default VMware repository URL that is preset for the build profile of the appliance. |
| **Use specified repository** | Uses a custom repository. You must enter the repository URL, for example, *`http://web_server_name.your_company.com`*`/vc_update_repo`.<br>If the repository policy requires authentication, enter a user name and password. |

5 Click **OK**.

### What to do next

Check for and Install vCenter Server Appliance Patches

## Check for and Install vCenter Server Appliance Patches

You can check for and install patches either from an ISO image or directly from a repository URL.

**Important** The services running in the appliance become unavailable during the installation of the patches. You must perform this procedure during a maintenance period. As a precaution in case of failure, you can back up the vCenter Server Appliance. For information on backing up and restoring vCenter Server, see *vSphere Installation and Setup*.

### Prerequisites

- Log in to the vCenter Server Appliance Management Interface as root.
- If you are patching the appliance from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server Appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Web Client. See *vSphere Virtual Machine Administration*.
- If you are patching the appliance from a repository URL, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure the Repository for URL-Based Patching.
- If you are patching a vCenter Server Appliance with an external Platform Services Controller, verify that you have applied the patches to the Platform Services Controller and its replicating partners, if any in the vCenter Single Sign-On domain.

### Procedure

1. In the vCenter Server Appliance Management Interface, click **Update**.

   In the Current version details pane, you can view the vCenter Server Appliance version and build number. You can also view the history of installed patches, if any.

2. Click **Check Updates** and select a source.

| Option | Description |
|---|---|
| **Check URL** | Scans the configured repository URL for available patches |
| **Check CDROM** | Scans the ISO image that you attached to the CD/DVD drive of the appliance for available patches |

   In the Available updates pane, you can view the details about the available patches in the source that you selected.

   **Important** Some updates might require a reboot of the system. You can see information about these updates in the Available updates pane.

3 Click **Install Updates** and select the range of patches to apply.

| Option | Description |
|---|---|
| **Install all updates** | Applies all available VMware and third-party patches |
| **Install third-party updates** | Applies only the third-party patches |

4 Read and accept the End User License Agreement.

5 After the installation completes, click **OK**.

6 If patch installation requires the appliance to reboot, click **Summary**, and click **Reboot** to reset the appliance.

#### Results

In the Available updates pane, you can see the changed update status of the appliance.

### Enable Automatic Checks for vCenter Server Appliance Patches

You can configure the vCenter Server Appliance to perform automatic checks for available patches in the configured repository URL at a regular interval.

#### Prerequisites

- Log in to the vCenter Server Appliance Management Interface as root.
- Verify that you have configured the repository settings and that the current repository URL is accessible. See Configure the Repository for URL-Based Patching.

#### Procedure

1 In the vCenter Server Appliance Management Interface, click **Update**.

2 Click **Settings**.

3 Select **Check for updates automatically**, and select the day and time in UTC to perform automatic checks for available patches.

4 Click **OK**.

#### Results

The appliance performs regular checks for available patches in the configured repository URL. In the Available updates pane, you can view information about the available patches. You can also view the vCenter Server Appliance health status for notifications about available patches. See *vCenter Server Appliance Configuration*.

## Patching the vCenter Server Appliance by Using the Appliance Shell

You can use the `software-packages` utility in the appliance shell of a vCenter Server Appliance that contains a vCenter Server with an embedded Platform Services Controller, a vCenter Server with an external Platform Services Controller, or a Platform Services Controller to see the installed patches, stage new patches, and install new patches.

To perform ISO-based patching, you download an ISO image, attach the ISO image to the CD/DVD drive of the appliance, optionally stage the available patches from the ISO image to the appliance, and install the patches.

To perform URL-based patching, you optionally stage the available patches from a repository URL to the appliance and install the patches. The vCenter Server Appliance is preset with a default VMware repository URL for the build profile of the appliance. You can use the `update.set` command to configure the appliance to use the default VMware repository URL or a custom repository URL, for example, a repository URL that you previously built on a local Web server running within your data center. You can also use the `proxy.set` command to configure a proxy server for the connection between the vCenter Server Appliance and the repository URL.

## View a List of All Installed Patches in the vCenter Server Appliance

You can use the `software-packages` utility to see a list of the patches currently applied to the vCenter Server Appliance. You can also view the list of the installed patches in chronological order and details about a specific patch.

### Procedure

1. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.

2. To view the full list of patches and software packages installed in the vCenter Server Appliance, run the following command:

   ```
   software-packages list
   ```

3. To view all patches applied to the vCenter Server Appliance in chronological order, run the following command:

   ```
   software-packages list    --history
   ```

   You see the list in chronological order. A single patch in this list can be an update of multiple different packages.

4. To view details about a specific patch, run the following command:

   ```
   software-packages list --patch    patch_name
   ```

   For example, if you want to view the details about the VMware-vCenter-Server-Appliance-Patch1 patch, run the following command:

   ```
   software-packages list --patch VMware-vCenter-Server-Appliance-Patch1
   ```

   You can see the complete list of details about the patch, such as vendor, description, and installation date.

## Configure URL-Based Patching

For URL-based patching, the vCenter Server Appliance is preset with a default VMware repository URL for the build profile of the appliance. You can use the `update.set` command to configure the appliance to use the default or a custom repository URL as the current source of patches and enable automatic checks for patches.

By default the current repository for URL-based patching is the default VMware repository URL.

**Note** You can use the `proxy.set` command to configure a proxy server for the connection between the vCenter Server Applianceand the repository URL. For more information about the API commands in the appliance shell, see *vCenter Server Appliance Configuration*.

If the vCenter Server Appliance is not connected to the Internet or if your security policy requires it, you can build and configure a custom repository that runs on a local Web server within your data center and replicates the data from the default VMware repository URL. Optionally, you can set up authentication policy for accessing the Web server that hosts the custom patching repository.

### Procedure

1. If you want to configure a custom repository URL, build the repository on your local Web server.
   a. Download the vCenter Server Appliance patch ZIP file from the VMware Web site at https://my.vmware.com/web/vmware/downloads.
   b. On your Web server, create a repository directory under the root.

      For example, create the **`vc_update_repo`** directory.
   c. Extract the ZIP file into the repository directory.

      The extracted files are in the `manifest` and `package-pool` subdirectories.
2. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.
3. To see information about the current URL-based patching settings, run the `update.get` command.

   You can see information about the current repository URL, the default repository URL, the time at which the appliance last checked for patches, the time at which the appliance last installed patches, and the current configuration of automatic checks for patches.
4. Configure the current repository for URL-based patching.
   - To configure the appliance to use the default VMware repository URL, run the following command:

     ```
     update.set --currentURL default
     ```

- To configure the appliance to use a custom repository URL, run the following command:

  ```
  update.set --currentURL http://web_server_name.your_company.com/vc_update_repo [--username username] [--password password]
  ```

  where the square brackets [] enclose the command options.

  If the custom repository requires authentication, use the `--username username` and `--password password` options.

5 To enable automatic checks for vCenter Server Appliance patches in the current repository URL at regular intervals, run the following command:

```
update.set    --CheckUpdates enabled [--day    day] [--time    HH:MM:SS]
```

where the square brackets [] enclose the command options.

Use the `--day day` option to set the day for performing the regular checks for patches. You can set a particular day of the week, for example, `Monday`, or `Everyday`. The default value is `Everyday`.

Use the `--time HH:MM:SS` option to set the time in UTC for performing the regular checks for patches. The default value is `00:00:00`.

The appliance performs regular checks for available patches in the current repository URL.

6 To disable automatic checks for vCenter Server Appliance patches, run the following command:

```
update.set    --CheckUpdates disabled
```

#### What to do next

If you configured the appliance to perform automatic checks for available patches, you can regularly view the vCenter Server Appliance health status for notifications about available patches. See *vCenter Server Appliance Configuration*.

## Stage Patches to the vCenter Server Appliance

Before you install available patches, you can stage the patches to the appliance. You can use the `software-packages` utility to stage patches either from a local repository by attaching an ISO image to the appliance, or from a remote repository directly by using a repository URL.

#### Prerequisites

- If you are staging patches from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server Appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Web Client. See *vSphere Virtual Machine Administration*.

- If you are staging patches from a remote repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.

**Procedure**

1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

2 Stage the patches.

- To stage the patches included in the attached ISO image, run the following command:

```
software-packages stage --iso
```

- To stage the patches included in the current repository URL, run the following command:

```
software-packages stage --url
```

By default the current repository URL is the default VMware repository URL.

If you want to stage only the third-party patches, use the `--thirdParty` option.

- To stage the patches included in a repository URL that is not currently configured in the appliance, run the following command:

```
software-packages stage --url URL_of_the_repository
```

If you want to stage only the third-party patches, use the `--thirdParty` option.

If you want to directly accept the End User License Agreement, use the `--acceptEulas` option.

For example, to stage only the third-party patches from the current repository URL with directly accepting the End User License Agreement, run the following command:

```
software-packages stage --url --thirdParty --acceptEulas
```

In the process of staging, the command validates that a patch is a VMware patch, that the staging area has enough free space, and that the patches are not altered. Only completely new patches or patches for existing packages that can be upgraded are staged.

3 (Optional) To see information about the staged patches, run the following command:

```
software-packages list    --staged
```

Each patch includes a metadata file that contains information such as patch version, product name, whether a restart of the system is required, and so on.

4 (Optional) To view a list of the staged patches, run the following command:

```
software-packages list --staged --verbose
```

5 (Optional) To unstage the staged patches, run the following command:

```
software-packages    unstage
```

All directories and files generated by the staging process are removed.

#### What to do next

Install the staged patches. See Install vCenter Server Appliance Patches.

**Important** If you staged the patches from an ISO image, keep the ISO image attached to the CD/DVD drive of the appliance. The ISO image must be attached to the CD/DVD drive of the appliance throughout the staging and installation processes.

## Install vCenter Server Appliance Patches

You can use the `software-packages` utility to install the staged patches. You can also use the `software-packages` utility to install patches directly from an attached ISO image or repository URL without staging the patch payload.

**Important** The services running in the appliance become unavailable during the installation of the patches. You must perform this procedure during a maintenance period. As a precaution in case of failure, you can back up the vCenter Server Appliance. For information about backing up and restoring vCenter Server, see *vSphere Installation and Setup*.

#### Prerequisites

- If you are installing staged patches, verify that you staged the correct patch payload. See Stage Patches to the vCenter Server Appliance.
- If you are installing patches that you previously staged from an ISO image, verify that the ISO image is attached to the CD/DVD drive of the vCenter Server Appliance. See Stage Patches to the vCenter Server Appliance.
- If you are installing patches directly from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server Appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Web Client. See *vSphere Virtual Machine Administration*.
- If you are installing patches directly from a repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.
- If you are patching a vCenter Server Appliance with an external Platform Services Controller, verify that you have applied the patches to the Platform Services Controller and its replicating partners, if any in the vCenter Single Sign-On domain.

Procedure

1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

2 Install the patches.

- To install staged patches, run the following command:

```
software-packages install --staged
```

- To install patches directly from an attached ISO image, run the following command:

```
software-packages install --iso
```

- To install patches directly from the current repository URL, run the following command:

```
software-packages install --url
```

By default the current repository URL is the default VMware repository URL.

If you want to install only the third-party patches, use the `--thirdParty` option.

- To install patches directly from a repository URL that is not currently configured, run the following command:

```
software-packages install --url URL_of_the_repository
```

If you want to install only the third-party patches, use the `--thirdParty` option.

If you want to directly accept the End User License Agreement, use the `--acceptEulas` option.

For example, to install only the third-party patches from the current repository URL without staging the patches with directly accepting the End User License Agreement, run the following command:

```
software-packages install --url    --thirdParty --acceptEulas
```

3 If the patch installation requires a reboot of the appliance, run the following command to reset the appliance.

```
shutdown reboot -r "patch reboot"
```

# After Upgrading vCenter Server 6

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

- You can review the database upgrade logs. See Collect Database Upgrade Logs.
- Complete any component reconfigurations that might be required for changes during upgrade.
- Verify that you understand the authentication process and identify your identity sources.
- Upgrade any additional modules that are linked to this instance of vCenter Server, such as vSphere Update Manager.
- Optionally, upgrade or migrate the ESXi hosts in the vCenter Server inventory to the same version as the vCenter Server instance.

This chapter includes the following topics:

# Complete vCenter Server Postupgrade Component Configuration

Complete the post-upgrade options and requirements that apply to your configuration.

If you have a local Auto Deploy service registered to vCenter Server before upgrade, it is upgraded automatically and there is no change of location. If you have a remote Auto Deploy service registered to vCenter Server before upgrade, it is migrated to the machine where vCenter Server is located when it is upgraded.

If you have a vSphere Web Client service registered to vCenter Server before upgrade, it is upgraded automatically and there is no change of location. If you have a remote vSphere Web Client registered to vCenter Server before upgrade, it is migrated to the machine where vCenter Server is located when it is upgraded.

For information on repointing previously distributed component services that are migrated to the vCenter Server physical server or virtual machine during upgrade, see Reconfigure Migrated vCenter Server Services After Upgrade.

SSL certification checking is required to configure vSphere HA on the hosts.

**Procedure**

1. On the VMware Web site, log in to your account page to access the license portal. From the license portal, upgrade your vCenter Server license. Using the vSphere Web Client, assign the upgraded license key to the vCenter Server host.
2. For Oracle databases, copy the Oracle JDBC Driver (`ojdbc14.jar` or `ojdbc5.jar`) to the `[VMware vCenter Server]\tomcat\lib` folder.
3. For Microsoft SQL Server databases, if you enabled bulk logging for the upgrade, disable it after the upgrade is complete.
4. If you have vSphere HA clusters, SSL certificate checking must be enabled.

   If certificate checking is not enabled when you upgrade, vSphere HA fails to configure on the hosts.

   a. Select the vCenter Server instance in the inventory panel.

   b. Select the **Manage** tab and the **General** subtab.

   c. Verify that the **SSL settings** field is set to **vCenter Server requires verified host SSL certificates**.

# Reconfigure Migrated vCenter Server Services After Upgrade

vCenter Server 5.x services that were previously deployed separately from vCenter Server might require reconfiguration after they are migrated to the vCenter Server system during the upgrade process.

vCenter Server components can no longer be deployed separately. If components of vCenter Server 5.x were previously deployed in different systems from the vCenter Server system, the upgrade software migrates them to the vCenter Server system. In some cases, repointing or other actions are required for the migrated services.

For vCenter Server Appliance 5.5 instances with remote relay of logs to external receivers such as LogInsight or Splunk, the upgrade software migrates the relay configuration to the VMware Syslog Service that is included in vCenter Server Appliance 6.0.

When you are upgrading in a mixed-version environment, vCenter Server 5.x instances that were using the vCenter Single Sign-On instance are not affected. They continue to operate with the upgraded Platform Services Controller instance as they did before the upgrade without any issues or required updates. vCenter Server 5.5 instances continue to be visible to version 5.5 vSphere Web Client, but not to version 6.0 vSphere Web Client instances. See Mixed-Version Transitional Environments During vCenter Server Upgrades.

**Procedure**

1. If your vSphere Auto Deploy service was previously installed on a separate machine from vCenter Server, and was relocated during the upgrade process, update your DHCP and TFTP settings to point to your relocated vSphere Auto Deploy service.
   a. Download `deploy-tftp.zip` and replace the tftp root folder.

      Your configuration can vary based on your TFTP client.

   b. Reconfigure the DHCP `.conf` file to use the upgraded vSphere Auto Deploy service and its `.tramp` file.

      Your configuration can vary based on your DHCP setup.
2. If your vSphere Web Client was previously installed on a separate machine from vCenter Server and was relocated during the upgrade process, update the FQDN and IP address to point to the new location.
3. If your VMware vSphere Syslog Collector was previously installed on a separate machine from vCenter Server, repoint ESXi hosts to the new location of the vSphere Syslog Collector server, which is the newly upgraded vCenter Server 6.0 for Windows.
4. If your vSphere ESXi Dump Collector server was previously installed on a separate machine from vCenter Server, repoint ESXi hosts to the new location of the vSphere ESXi Dump Collector server.
5. To apply the configuration changes for the remote relay of logs to the vSphere Syslog Service service in an upgraded vCenter Server Appliance, restart the service immediately after the upgrade to 6.0 is completed.
6. To view any vCenter Server 5.5 instances that are not yet upgraded while you have a transitional mixed-version 5.5 and 6.0 environment, restart your legacy vSphere Web Client.

7 If any vCenter Server 5.x services remain running on separate virtual machines or physical servers, you can shut down and remove them.

They are not used by vCenter Server 6.0.

# 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.

### Results

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.

# Upgrade the vSphere Client

Virtual machine users and vCenter Server administrators must use the vSphere Client 6.0 to connect to vCenter Server 6.0 or to connect directly to ESXi 6.0 hosts.

You can install the VI Client 2.5, the vSphere Client 4.x, the vSphere Client 5.x, and the vSphere Client 6.0 on the same machine. After you upgrade vCenter Server, upgrade the vSphere Client to the same version to avoid compatibility problems that might interfere with the operation of the vSphere Client.

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

### Prerequisites

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

### Procedure

1 (Optional) Use **Add/Remove Programs** from the Windows Control Panel to remove any previous vCenter Server client.

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

2 Run the vSphere Client installer.

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

### Results

After you install the vSphere Client 6.0, you can connect to an ESXi host by using the domain name or IP address of the host and the user name and password of a user on that machine.

### What to do next

Use the vSphere Client to connect directly to an ESXi host by using your user name and password.

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

# Configuring VMware vCenter Server - tc Server Settings in vCenter Server

Starting with vCenter Server 5.1, VMware Tomcat Server settings can no longer be configured through the Windows user interface. vCenter Server versions 5.1 and later use VMware vCenter Server - tc Server, an enterprise version of Apache Tomcat 7. Tomcat version 7 does not provide a control panel in the Windows user interface. Instead, you configure Tomcat by editing configuration files manually.

Settings for Java options are stored in the following files.

- vCenter Server.
  *`installation_directory`*`\VMware\Infrastructure\tomcat\conf\wrapper.conf`
- vCenter Inventory Service.
  *`installation_directory`*`\VMware\Infrastructure\Inventory Service\conf\wrapper.conf`

- Profile-Driven Storage Service. *installation_directory*\VMware\Infrastructure\Profile-Driven Storage\conf\wrapper.conf
- vSphere Web Client. *installation_directory*\VMware\vSphereWebClient\server\bin\service\conf\wrapper.conf

### Table 6-1. JVM Heap Size Setting for Inventory Service and Profile-Driven Storage Service, with Java Maximum n the `wrapper.conf` Files

| Java Option | Setting and Default Value |
|---|---|
| `maxmemory`*size*<br>The maximum JVM heap size, in megabytes. This setting controls the maximum size of the Java heap. Tuning this parameter can reduce the overhead of garbage collection, improving server response time and throughput. For some applications, the default setting for this option is too low, resulting in a high number of minor garbage collections. | Inventory Service: `wrapper.java.maxmemory=2048`<br>Profile-Driven Storage Service: `wrapper.java.maxmemory=1024`<br>The vSphere Web Client: For large deployments you might need to set this option to `wrapper.java.maxmemory=2048` . |
| `ping.timeout`*duration* | The vSphere Web Client: For large deployments you might need to set this option to `wrapper.ping.timeout=120`. |

vCenter Server security and port settings are stored in the following files.

- *installation_directory*\VMware\Infrastructure\tomcat\conf\server.xml
- *installation_directory*\VMware\Infrastructure\tomcat\conf\catalina.properties

### Table 6-2. vCenter Server Port and Security Settings in the `server.xml` and `catalina.properties` Files

| vCenter Server Port or Security Setting | Setting and Default Value |
|---|---|
| Base shutdown port | base.shutdown.port=8003 |
| Base JMX port. The listener implemented by the com.springsource.tcserver.serviceability.rmi.JmxSocketListener class is specific to tc Server. This listener enables JMX management of tc Server, and is the JMX configuration that the AMS management console uses to manage tc Server instances. The port attribute specifies the port of the JMX server that management products, such as AMS, connect to. The *${jmx.port}* variable is set to 6969 in the default `catalina.properties` file. The bind attribute specifies the host of the JMX server. By default, this attribute is set to the localhost (127.0.0.1).<br>The default -1 setting disables the port. | base.jmx.port=-1 |
| Web services HTTPS | bio-vmssl.http.port=8080 |
| Web services HTTPS | bio-vmssl.https.port=8443 |

Table 6-2. vCenter Server Port and Security Settings in the `server.xml` and `catalina.properties` Files (continued)

| vCenter Server Port or Security Setting | Setting and Default Value |
|---|---|
| SSL certificate | bio-vmssl.keyFile.name=C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.pfx |
| SSL certificate password | bio-vmssl.SSL.password=testpassword |

See *Getting Started with vFabric tc Server* and *vFabric tc Server Administration* at https://www.vmware.com/support/pubs/vfabric-tcserver.html.

You can manage the Windows services for vCenter Server from the Administrative Tools control panel, under Services. The Windows service for vCenter Server is listed as VMware VirtualCenter Management Webservices.

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

By default, a vCenter Server creates a maximum of 50 simultaneous database connections. If you configure this value to less than 50 in the previous version of vCenter Server and then perform the upgrade to vCenter Server 5.x, the upgrade restores the default setting of 50. If you configure this value to more than 50 in the previous version of vCenter Server, after the upgrade to vCenter Server 5.x, the system retains the previous value. You can reconfigure the nondefault setting.

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

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

### Procedure

1. From the vSphere Web Client, connect to the vCenter Server.
2. Select the vCenter Server in the inventory.
3. Click the **Manage** tab.
4. Select **Settings**.
5. Select **General**.
6. Click **Edit**.
7. Select **Database**.
8. Change the **Maximum connections** value as appropriate.
9. Click **OK**.

10 Restart the vCenter Server.

**Results**

The new database setting takes effect.

# 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*.

# 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*.

# Restore ESXi Certificate and Key Files

When you replace a certificate on an ESXi host by using the vSphere Web Services SDK, the previous certificate and key are appended to a `.bak` file. You can restore previous certificates by moving the information in the `.bak` file to the current certificate and key files.

The host certificate and key are located in `/etc/vmware/ssl/rui.crt` and `/etc/vmware/ssl/rui.key`. When you replace a host certificate and key by using the vSphere Web Services SDK `vim.CertificateManager` managed object, the previous key and certificate are appended to the file `/etc/vmware/ssl/rui.bak`.

**Note** If you replace the certificate by using HTTP PUT, `vifs`, or from the ESXi Shell, the existing certificates are not appended to the `.bak` file.

### Procedure

1 On the ESXi host, locate the file `/etc/vmware/ssl/rui.bak`.

  The file has the following format.

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#
```

```
-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2 Copy the text starting with `-----BEGIN PRIVATE KEY-----` and ending with `-----END PRIVATE KEY-----` into the `/etc/vmware/ssl/rui.key` file.

   Include `-----BEGIN PRIVATE KEY-----` and `-----END PRIVATE KEY-----`.

3 Copy the text between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` into the `/etc/vmware/ssl/rui.crt` file.

   Include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

4 Restart the host or send `ssl_reset` events to all services that use the keys.

   ```
   for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s ssl_reset; fi; done
   ```

# Repoint vCenter Server to Another External Platform Services Controller

Joining external Platform Services Controller instances in the same vCenter Single Sign-On domain, ensures high availability of your system.

If an external Platform Services Controller stops responding or if you want to distribute the load of an external Platform Services Controller, you can repoint the vCenter Server instances to another Platform Services Controller in the same domain and site.

- You can repoint the vCenter Server instance to an existing functional Platform Services Controller instance with free load capacity in the same domain and site.
- You can install or deploy a new Platform Services Controller instance in the same domain and site to which to repoint the vCenter Server instance.

### Prerequisites

- If the old Platform Services Controller instance has stopped responding, remove the node and clean up the stale vmdir data by running the `cmsso-util unregister` command. For information about decommissioning a Platform Services Controller instance, see https://kb.vmware.com/kb/2106736.
- Verify that the old and the new Platform Services Controller instances are in the same vCenter Single Sign-On domain and site by running the `vdcrepadmin -f showservers` command. For information about using the command, see https://kb.vmware.com/kb/2127057.

### Procedure

1 Log in to the vCenter Server instance.

- For a vCenter Server Appliance, log in to the vCenter Server Appliance shell as root.
- For a vCenter Server instance on Windows, log in as an administrator to the vCenter Server virtual machine or physical server.

2 If the vCenter Server instance runs on Windows, in the Windows command prompt, navigate to `C:\Program Files\VMware\vCenter Server\bin`.

3 Run the `cmsso-util repoint` command.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

where the square brackets [ ] enclose the command options.

Here, *psc_fqdn_or_static_ip* is the system name used to identify the Platform Services Controller. This system name must be an FQDN or a static IP address.

**Note** The FQDN value is case-sensitive.

Use the `--dc-port port_number` option if the Platform Services Controller runs on a custom HTTPS port. The default value of the HTTPS port is 443.

4 Log in to the vCenter Server instance by using the vSphere Web Client to verify that the vCenter Server is running and can be managed.

### Results

The vCenter Server instance is registered with the new Platform Services Controller.

## Reconfigure a Standalone vCenter Server with an Embedded Platform Services Controller to a vCenter Server with an External Platform Services Controller

If you have deployed or installed a standalone vCenter Server instance with an embedded Platform Services Controller and you want to extend your vCenter Single Sign-On domain with more vCenter Server instances, you can reconfigure and repoint the existing vCenter Server instance to an external Platform Services Controller.

Figure 6-1. Reconfiguration of a Standalone vCenter Server Instance with an Embedded Platform Services Controller and Repointing it to an External Platform Services Controller

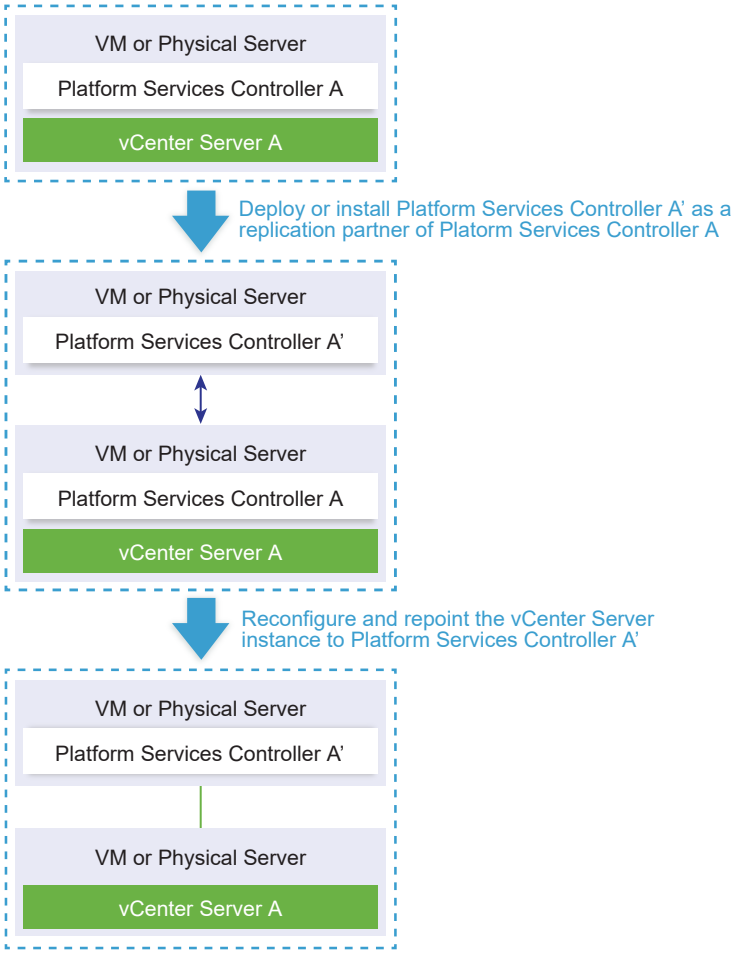



Table 6-3. Legend

| Arrow or line | Description |
|---|---|
| ↔ | Replication agreement between two Platform Services Controller instances |
| — | vCenter Server registration with an external Platform Services Controller |
| ↓ | Transition step |

**Note** The reconfiguration of a vCenter Server instance with an embedded Platform Services Controller and repointing it to an external Platform Services Controller instance is a one-way process after which you cannot switch back to vCenter Server with an embedded Platform Services Controller.

### Prerequisites

- Deploy or install the external Platform Services Controller instance as a replication partner of the existing embedded Platform Services Controller instance in the same vCenter Single Sign-On site.

  **Note** You can determine the current vCenter Single Sign-On site by using the `vmfad-cli` command.

  - For a vCenter Server Appliance with an embedded Platform Services Controller, log in to the appliance shell as root and run the command.

    ```
    /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
    ```

  - For a Windows installation of vCenter Server instance with an embedded Platform Services Controller, log in to the Windows machine as an administrator, open the Windows command prompt, and run the command.

    ```
    C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
    ```

- Create snapshots of the vCenter Server with an embedded Platform Services Controller and the external Platform Services Controller instance, so that you can revert to the snapshots if the reconfiguration fails.

### Procedure

1 Log in to the vCenter Server instance with an embedded Platform Services Controller.

| Option | Steps |
|---|---|
| For a vCenter Server Appliance with an embedded Platform Services Controller | Log in to the appliance shell as root.<br>■ If you have direct access to the appliance console, press Alt+F1.<br>■ If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance. |
| For a Windows installation of vCenter Server with an embedded Platform Services Controller | Log in to the Windows machine as an administrator. |

2 Verify that all Platform Services Controller services are running.

| Option | Steps |
|---|---|
| For a vCenter Server Appliance with an embedded Platform Services Controller | Run the `service-control --status --all` command. |
| For a Windows installation of vCenter Server with an embedded Platform Services Controller | Select **Start > Control Panel > Administrative Tools > Services**. |

The Platform Services Controller services that must be running are VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service, and VMware Directory Service.

3 If the vCenter Server with an embedded Platform Services Controller instance runs on Windows, open the Windows command prompt and navigate to `C:\Program Files\VMware\vCenter Server\bin`.

4 Run the `cmsso-util reconfigure` command.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --
domain-name domain_name --passwd password [--dc-port port_number]
```

where the square brackets [ ] enclose optional items.

Here, *psc_fqdn_or_static_ip* is the system name used to identify the external Platform Services Controller instance. This system name must be an FQDN or a static IP address.

**Note** The FQDN value is case-sensitive.

The options *username* and *password* are the administrator user name and password of the vCenter Single Sign-On *domain_name*.

Use the `--dc-port` option if the external Platform Services Controller runs on a custom HTTPS port. The default value of the HTTPS port is 443.

For example, if the external Platform Services Controller runs on a custom HTTPS port 449, you must run:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --
domain-name vsphere.local --passwd Password1! --dc-port 449
```

5 Log in to the vCenter Server instance by using the vSphere Web Client to verify that the vCenter Server is running and can be managed.

### Results

The vCenter Server with an embedded Platform Services Controller is demoted, and the vCenter Server is redirected to the external Platform Services Controller.

### What to do next

You can deploy or install additional vCenter Server and Platform Services Controller instances in the vCenter Single Sign-On domain.

## Reconfigure Multiple Joined Instances of vCenter Server with an Embedded Platform Services Controller to vCenter Server with an External Platform Services Controller

If you have deployed or installed two or more joined instances of vCenter Server with an embedded Platform Services Controller, you can reconfigure them as multiple vCenter Server instances that are using joined external Platform Services Controller instances.

Figure 6-2. Example Reconfiguration of Three Joined Instances of vCenter Server with an Embedded Platform Services Controller Across Two vCenter Single Sign-On Sites

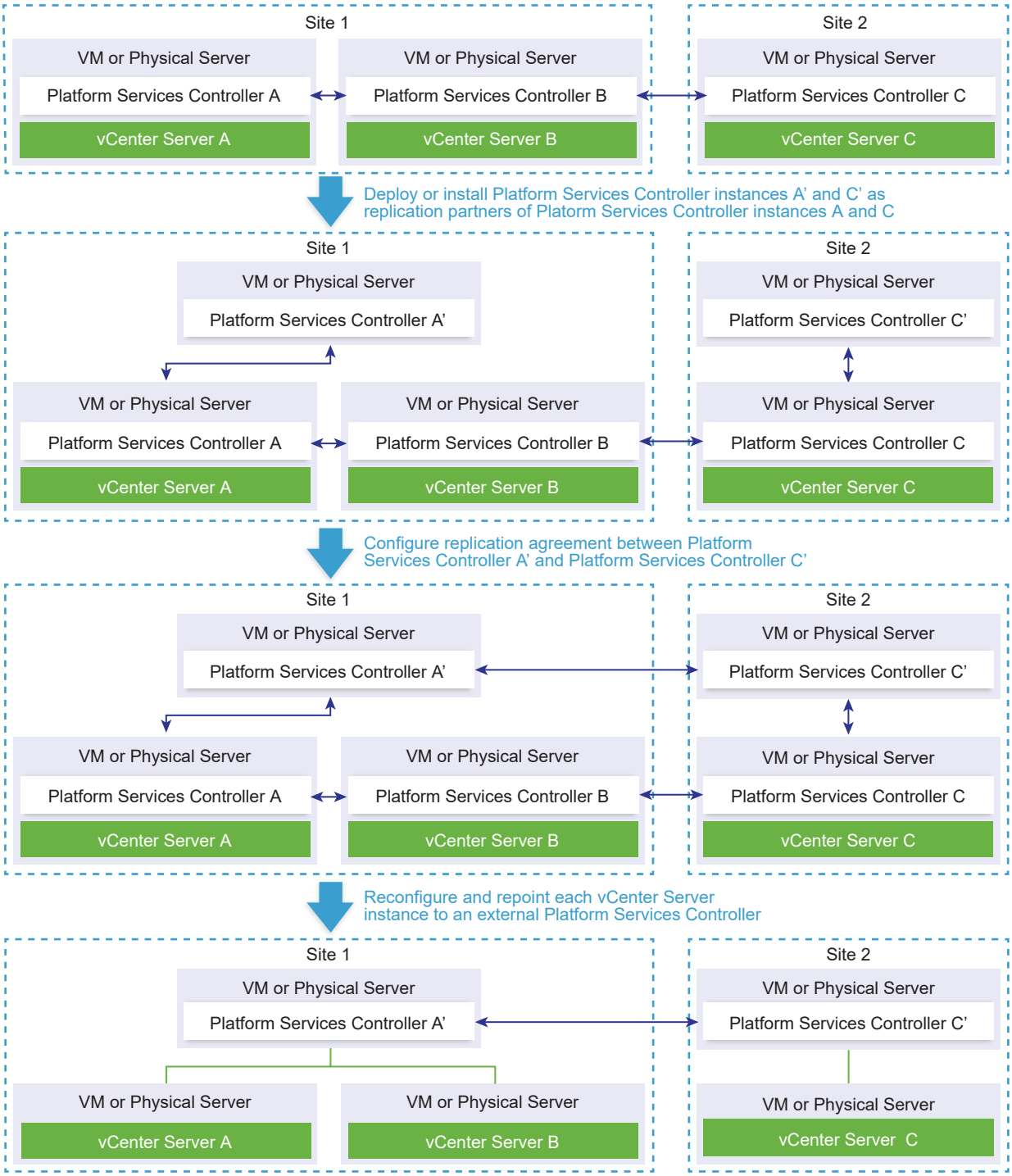


Table 6-4. Legend

| Arrow or line | Description |
| --- | --- |
|  | Replication agreement between two Platform Services Controller instances |
|  | vCenter Server registration with an external Platform Services Controller |
|  | Transition step |

**Note** The reconfiguration of a vCenter Server instance with an embedded Platform Services Controller and repointing it to an external Platform Services Controller instance is a one-way process after which you cannot switch back to vCenter Server with an embedded Platform Services Controller.

**Prerequisites**

- For each vCenter Single Sign-On site, deploy or install an external Platform Services Controller instance as a replication partner of an existing embedded Platform Services Controller instance from this site.

  **Note** You can determine the current vCenter Single Sign-On sites by using the `vmfad-cli` command.

  - For a vCenter Server Appliance with an embedded Platform Services Controller, log in to the appliance shell as root and run the command.

    ```
    /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
    ```

  - For a Windows installation of vCenter Server instance with an embedded Platform Services Controller, log in to the Windows machine as an administrator, open the Windows command prompt, and run the command.

    ```
    C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
    ```

- Create snapshots of the vCenter Server instances with an embedded Platform Services Controller and the external Platform Services Controller instances, so that you can revert to the snapshots if the reconfiguration fails.

## Verify that the Services of the Embedded Platform Services Controller Instances are Running

To ensure a successful repointing of a vCenter Server instance from an embedded to an external Platform Services Controller, all services of the existing embedded Platform Services Controller instance must be running.

Procedure

1 Log in to a vCenter Server instance with an embedded Platform Services Controller.

| Option | Steps |
| --- | --- |
| For a vCenter Server Appliance with an embedded Platform Services Controller | Log in to the appliance shell as root.<br>■ If you have direct access to the appliance console, press Alt+F1.<br>■ If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance. |
| For a Windows installation of vCenter Server with an embedded Platform Services Controller | Log in to the Windows machine as an administrator. |

2 Verify that all Platform Services Controller services are running.

| Option | Steps |
| --- | --- |
| For a vCenter Server Appliance with an embedded Platform Services Controller | Run the `service-control --status --all` command. |
| For a Windows installation of vCenter Server with an embedded Platform Services Controller | Select **Start > Control Panel > Administrative Tools > Services**. |

The Platform Services Controller services that must be running are VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service, and VMware Directory Service.

3 Repeat this procedure for each vCenter Server instance with an embedded Platform Services Controller.

## Configure Replication Agreement Between All External Platform Services Controller Instances

After you have deployed or installed an external replicating Platform Services Controller instance in each vCenter Single Sign-On site, you must join all external Platform Services Controller instances in replication agreement.

Figure 6-3. Example Configuration of Replication Agreement Between Two External Platform Services Controller Instances in Different vCenter Single Sign-On Sites

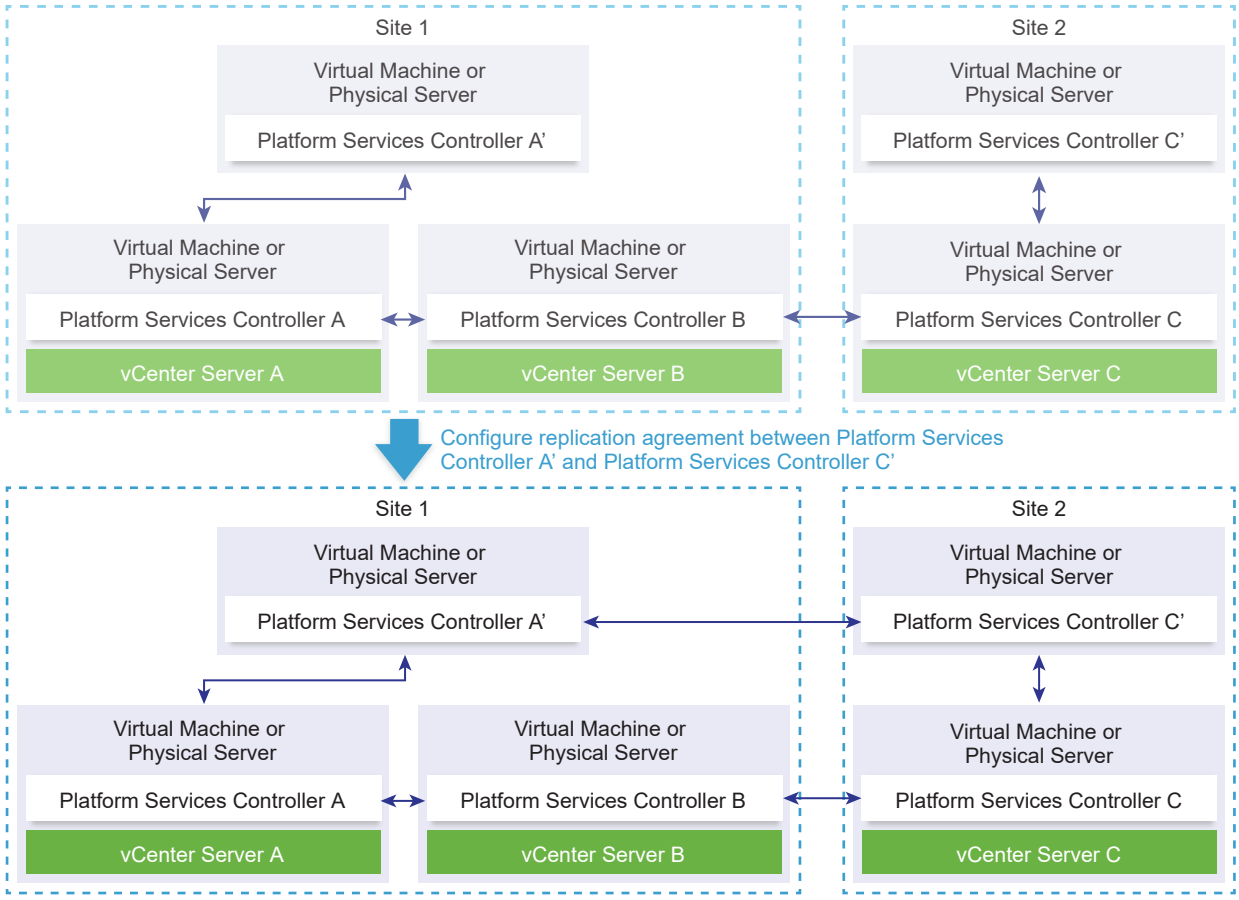



Table 6-5. Legend

| Arrow or line | Description |
|---|---|
| ↔ | Replication agreement between two Platform Services Controller instances |
| — | vCenter Server registration with an external Platform Services Controller |
| ↓ | Transition step |

To configure replication agreement between two Platform Services Controller instances, you can use a connection to any of the vCenter Server or Platform Services Controller instances from the vCenter Single Sign-On domain.

Procedure

1 Connect to a vCenter Server or Platform Services Controller instance from the vCenter Single Sign-On domain.

| Option | Steps |
| --- | --- |
| If you want to connect to a vCenter Server Appliance or Platform Services Controller appliance | Log in to the appliance Bash shell as root.<br>1 Log in to the appliance shell<br>■ If you have direct access to the appliance console, press Alt+F1.<br>■ If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance.<br>2 Enable the Bash shell<br>`shell.set --enabled true`<br>3 Run the `shell` command. |
| If you want to connect to a Windows installation of vCenter Server or Platform Services Controller | Log in to the Windows machine as an administrator and open the Windows command prompt. |

2 Run the `vdcrepadmin` command with the `showpartners` parameter against one external Platform Services Controller instance.

You determine the existing partnerships of the Platform Services Controller instance with other Platform Services Controller instances in the vCenter Single Sign-On domain.

- If you are using a connection to a vCenter Server Appliance or Platform Services Controller appliance, run the following command.

  `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h` *`psc_fqdn_or_static_ip`* `-u administrator`

- If you are using a connection to a Windows installation of vCenter Server or Platform Services Controller, run the following command.

  `C:\Program Files\VMware\vCenter Server\vmware-vmdir\bin\vdcrepadmin -f showpartners -h` *`psc_fqdn_or_static_ip`* `-u administrator`

When prompted, enter the vCenter Single Sign-On administrator password.

3 Repeat Step 2 against each external Platform Services Controller instance.

You determined the existing partnerships between all Platform Services Controller instances in the vCenter Single Sign-On domain.

4 If there is an external Platform Services Controller instance that is not in replication agreement with another external Platform Services Controller instance, run the `vdcrepadmin` command with the `createagreement` parameter against this Platform Services Controller instance to join it to another external Platform Services Controller instance.

- If you are using a connection to a vCenter Server Appliance or Platform Services Controller appliance, run the following command.

```
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h
psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u administrator
```

- If you are using a connection to a Windows installation of vCenter Server or Platform Services Controller, run the following command.

  ```
  C:\Program Files\VMware\vCenter Server\vmware-vmdir\bin\vdcrepadmin -f
  createagreement -2 -h psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u
  administrator
  ```

When prompted, enter the vCenter Single Sign-On administrator password.

You created a partnership between the two Platform Services Controller instances.

5 Repeat Step 4 against each external Platform Services Controller instance that is not in replication agreement with another external Platform Services Controller instance.

6 Repeat Step 2 and Step 3 to verify that you configured a ring partnership topology of the external Platform Services Controller instances.

## Reconfigure Each vCenter Server Instance and Repoint It from an Embedded to External Platform Services Controller Instance

With the reconfiguration you demote each embedded Platform Services Controller and redirect the vCenter Server instance to use an external Platform Services Controller instance.

Figure 6-4. Example Reconfiguration of Three Joined Instances of vCenter Server with an Embedded Platform Services Controller and Repointing Them to the External Platform Services Controller Instances

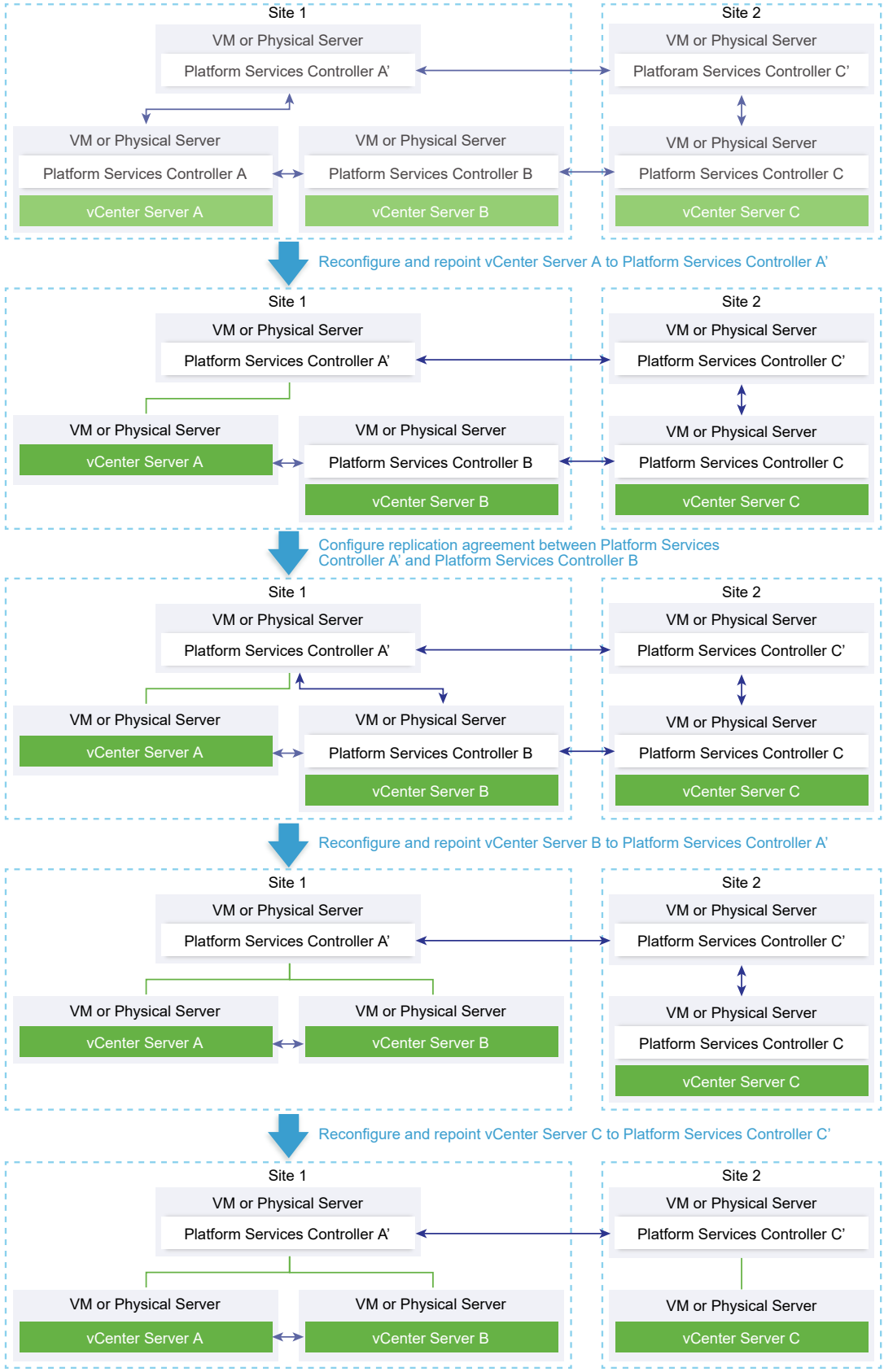


Table 6-6. Legend

| Arrow or line | Description |
| --- | --- |
|  | Replication agreement between two Platform Services Controller instances |
|  | vCenter Server registration with an external Platform Services Controller |
|  | Transition step |

Procedure

1 Log in to the vCenter Server instance with an embedded Platform Services Controller.

| Option | Steps |
| --- | --- |
| For a vCenter Server Appliance with an embedded Platform Services Controller | Log in to the appliance shell as root.<br>■ If you have direct access to the appliance console, press Alt+F1.<br>■ If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance. |
| For a Windows installation of vCenter Server with an embedded Platform Services Controller | Log in to the Windows machine as an administrator. |

2 If the vCenter Server with an embedded Platform Services Controller instance and the external Platform Services Controller instance are not direct replication partners, create such a replication agreement.

- For a vCenter Server Appliance with an embedded Platform Services Controller, from the appliance Bash shell, run the following command.

  ```
  /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -h localhost -H psc_fqdn_or_static_ip -u administrator
  ```

- For a Windows installation of vCenter Server with an embedded Platform Services Controller, from the Windows command prompt, run the following command.

  ```
  C:\Program Files\VMware\vCenter Server\vmware-vmdir\bin\vdcrepadmin -f createagreement -h localhost -H psc_fqdn_or_static_ip -u administrator
  ```

When prompted, enter the vCenter Single Sign-On administrator password.

3 If the vCenter Server with an embedded Platform Services Controller instance runs on Windows, in the Windows command prompt, navigate to `C:\Program Files\VMware\vCenter Server\bin`.

4 Run the `cmsso-util reconfigure` command.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --domain-name domain_name --passwd password [--dc-port port_number]
```

where the square brackets [ ] enclose optional items.

Here, *psc_fqdn_or_static_ip* is the system name used to identify the external Platform Services Controller instance. This system name must be an FQDN or a static IP address.

**Note** The FQDN value is case-sensitive.

The options *username* and *password* are the administrator user name and password of the vCenter Single Sign-On *domain_name*.

Use the `--dc-port` option if the external Platform Services Controller runs on a custom HTTPS port. The default value of the HTTPS port is 443.

For example, if the external Platform Services Controller runs on a custom HTTPS port 449, you must run:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --
domain-name vsphere.local --passwd Password1! --dc-port 449
```

**Important** If you repointed the vCenter Server instance to use an external Platform Services Controller instance that is in a different vCenter Single Sign-On site, you must move the vCenter Server instance to this vCenter Single Sign-On site. For information about moving vCenter Server between different vCenter Single Sign-On sites, see VMware knowledge base article Repointing the VMware vCenter Server 6.0 between sites in a vSphere Domain.

5 Log in to the vCenter Server instance by using the vSphere Web Client to verify that the vCenter Server is running and can be managed.

6 Repeat this procedure for each vCenter Server instance with an embedded Platform Services Controller.

### Results

The vCenter Server instances with an embedded Platform Services Controller are demoted, and the vCenter Server instances are redirected to the external Platform Services Controller instances.

# Upgrading Update Manager 7

You can upgrade to Update Manager 6.0 only from Update Manager version 5.x that are installed on a 64-bit operating system.

If you are running Update Manager of a version earlier than 5.x, or Update Manager that runs on a 32-bit platform, you cannot perform an in-place upgrade to Update Manager 6.0. You must use the data migration tool that is provided with Update Manager 5.0 installation media to upgrade your Update Manager system to Update Manager 5.0 running on a 64-bit operating system, and then perform an in-place upgrade from version 5.0 to version 6.0. For detailed information how to use the data migration tool, see the *Installing and Administering VMware vSphere Update Manager* documentation for Update Manager 5.0.

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

Previous versions of Update Manager use a 512-bit key and self-signed certificate and these are not replaced during upgrade. If you require a more secure 2048-bit key, you can either perform a fresh installation of Update Manager 6.0, or use the Update Manager Utility to replace the existing certificate.

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

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

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

The Java Components (JRE) required by Update Manager are installed or upgraded silently on the system when you install or upgrade Update Manager. Starting with Update Manager 5.5 update 1, you can upgrade the Java Components separately from an Update Manager upgrade procedure to a version of the Java Components that is released asynchronously from the Update Manager releases.

This chapter includes the following topics:



# Upgrade the Update Manager Server

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

The Update Manager 6.0 release allows upgrades from only Update Manager 5.x.

### Prerequisites

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

### Procedure

1 Upgrade vCenter Server to a compatible version.

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

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

2 In the software installer directory, double-click the `autorun.exe` file and select **vSphere Update Manager > Server**.

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

3 Select a language for the installer and click **OK**.

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

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

6 Read and accept the license agreement, and click **Next**.

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

If you deselect **Delete the old host upgrade files from the repository**, you retain files that you cannot use with Update Manager 6.0.

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

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

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

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

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

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

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

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

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

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

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

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

15 Click **Finish**.

#### Results

You upgraded the Update Manager server.

#### What to do next

Upgrade the Update Manager Client plug-in.

# Before Upgrading Hosts

8

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

This chapter includes the following topics:

- Best Practices for ESXi Upgrades
- Upgrade Options for ESXi 6.0
- Upgrading Hosts That Have Third-Party Custom VIBs
- Using Manually Assigned IP Addresses for Upgrades Performed with vSphere Update Manager
- Media Options for Booting the ESXi Installer
- Using Remote Management Applications
- Download the ESXi Installer

## Best Practices for ESXi Upgrades

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

For a successful ESXi upgrade, follow these best practices:

1 Make sure that you understand the ESXi upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.
   - If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Read Upgrade Options for ESXi 6.0 to understand the upgrade scenarios that are supported, and the options and tools that are available to perform the upgrade.
   - Read the VMware vSphere Release Notes for known installation issues.
2 Prepare the system for the upgrade.
   - Make sure that the current ESXi version is supported for the upgrade. See Upgrade Options for ESXi 6.0.

- Make sure that the system hardware complies with ESXi requirements. See Chapter 2 Upgrade Requirements and VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php. Check for system compatibility, I/O compatibility with network and host bus adapter (HBA) cards, storage compatibility, and backup software compatibility.
- Make sure that sufficient disk space is available on the host for the upgrade.
- If a SAN is connected to the host, detach the Fibre Channel system before continuing with the upgrade. Do not disable HBA cards in the BIOS.

3 Back up the host before performing an upgrade. If the upgrade fails, you can restore the host.

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

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

6 Apply a host's licenses. See Applying Licenses After Upgrading to ESXi 6.0.

7 Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. vSphere Syslog Collector is included as a service in vCenter Server 6.0 and can be used to collect logs from all hosts. See Required Free Space for System Logging. For information about setting up and configuring syslog and a syslog server, setting up syslog from the host profiles interface, and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

8 If the upgrade was unsuccessful and you backed up the host, you can restore the host.

# Upgrade Options for ESXi 6.0

VMware provides several ways to upgrade ESXi 5.x hosts to ESXi 6.0 hosts.

The details and level of support for an upgrade to ESXi 6.0 depend on the host to be upgraded and the upgrade method that you use. Verify support for the upgrade path from your current version of ESXi to the version to which you are upgrading. See VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

You can upgrade a ESXi 5.x host, asynchronously released driver or other third-party customizations, interactive upgrade from CD or DVD, scripted upgrade, or upgrade with vSphere Update Manager. When you upgrade an ESXi 5.x host that has custom VIBs to version 6.0, the custom VIBs are migrated. See Upgrading Hosts That Have Third-Party Custom VIBs.

Methods supported for direct upgrade to ESXi 6.0 are:

- vSphere Update Manager.
- Interactive upgrade from CD, DVD, or USB drive.
- Scripted upgrade.

- vSphere Auto Deploy. If the ESXi 5.x host was deployed by using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with an ESXi 6.0 image.
- The `esxcli` command.

**vSphere Update Manager**

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

**Upgrade interactively by using an ESXi installer ISO image on CD/DVD or USB flash drive**

You can run the ESXi 6.0 installer from a CD/DVD or USB flash drive to do an interactive upgrade. This method is appropriate for deployments with a small number of hosts. The installer works the same as for a fresh installation, but if you select a target disk that already contains an ESXi 5.0.x,ESXi 5.1.x, or ESXi 5.5.x installation, the installer upgrades the host to 6.0. The installer also gives you the option to migrate some existing host settings and configuration files and to preserve the existing VMFS datastore. See Upgrade Hosts Interactively.

**Perform a scripted upgrade**

You can upgrade hosts from ESXi 5.0.x, ESXi 5.1.x, and ESXi 5.5.x to ESXi 6.0 by running an update script for an efficient, unattended upgrade. Scripted upgrades provide an efficient way to deploy multiple hosts. You can use a script to upgrade ESXi from a CD, DVD, or USB flash drive, or by specifying a preboot execution environment (PXE) for the installer. You can also call a script from an interactive installation. See Installing or Upgrading Hosts by Using a Script.

**vSphere Auto Deploy**

After an ESXi 5.x host is deployed with vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host and reboot it with a new image profile. This profile contains an ESXi upgrade or patch, a host configuration profile, and optionally, third-party drivers or management agents that are provided by VMware partners. You can build custom images by using vSphere ESXi Image Builder CLI. See Using vSphere Auto Deploy to Reprovision Hosts .

**esxcli**

You can use the `esxcli` command-line utility for ESXi to upgrade ESXi 5.0.x hosts, ESXi 5.1.x hosts, or ESXi 5.5.x hosts to ESXi 6.0 hosts.

The `esxupdate` and `vihostupdate` utilities are not supported for ESXi 6.0 upgrades. See Upgrading Hosts by Using esxcli Commands .

# Upgrading Hosts That Have Third-Party Custom VIBs

A host can have custom vSphere installation bundles (VIBs) installed, for example, for third-party drivers or management agents. When you upgrade an ESXi 5.x host to ESXi 6.0, all supported custom VIBs are migrated, regardless of whether the VIBs are included in the installer ISO.

If the host or the installer ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the VIB that created the conflict. To upgrade the host, take one of the following actions:

- Remove the VIB that created the conflict from the host and retry the upgrade. If you are using vSphere Update Manager, select the option to remove third-party software modules during the remediation process. For more information, see the *Installing and Administering VMware vSphere Update Manager* documentation. You can also remove the VIB that created the conflict from the host by using `esxcli` commands. For more information, see Remove VIBs from a Host .
- Use the vSphere ESXi Image Builder CLI to create a custom installer ISO image that resolves the conflict. For more information about vSphere ESXi Image Builder CLI installation and usage, see the *vSphere Installation and Setup* documentation.

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

If you are using vSphere Update Manager to upgrade a host from ESXi 5.x to ESXi 6.0, you must use manually assigned IP addresses for the hosts. Manually assigned IP addresses are also called static IP addresses.

IP addresses that are requested by using Dynamic Host Configuration Protocol (DHCP) can cause problems during host upgrades that are performed with vSphere Update Manager. If a host loses its DHCP IP address during an upgrade or migration because the lease period configured on the DHCP server expires, vSphere Update Manager loses connectivity to the host. In this case, even if the host upgrade or migration is successful, vSphere Update Manager reports an upgrade or migration failure, because it cannot connect to the host. To prevent this scenario, use manually assigned IP addresses for the hosts.

# Media Options for Booting the ESXi Installer

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

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See Download and Burn the ESXi Installer ISO Image to a CD or DVD.
- Boot from a USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.
- PXE boot from the network. PXE Booting the ESXi Installer

- Boot from a remote location using a remote management application. See Using Remote Management Applications

## 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.

### 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.

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

**Note** The `ks.cfg` 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

- Linux machine with superuser access to it
- USB flash drive that can be detected by the Linux machine
- The ESXi ISO image, `VMware-VMvisor-Installer-`*`version_number`*`-`*`build_number`*`.x86_64.iso`, which includes the `isolinux.cfg` file
- Syslinux package

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 command for displaying the current log messages.

   ```
   tail -f /var/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 Enter `d` to delete partitions until they are all deleted.

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

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

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

   e Enter `p` to print the partition table.

   The result should be similar to the following message.

   ```
   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 Enter `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 Install the Syslinux bootloader on the USB flash drive.

   The locations of the Syslinux executable file and the `mbr.bin` file might vary for the different Syslinux versions. For example, if you downloaded Syslinux 6.02, run the following commands.

```
/usr/bin/syslinux /dev/sdb1
cat /usr/lib/syslinux/mbr/mbr.bin > /dev/sdb
```

5 Create a destination directory and mount the USB flash drive to it.

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

6 Create a destination directory and mount the ESXi installer ISO image to it.

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

7 Copy the contents of the ISO image to the USB flash drive.

```
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, edit the `APPEND -c boot.cfg` line to `APPEND -c boot.cfg -p 1`.

10 Unmount the USB flash drive.

```
umount /usbdisk
```

11 Unmount the installer ISO image.

```
umount /esxi_cdrom
```

**Results**

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.

### Results

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 and About PXE Configuration Files.

## 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 and About the boot.cfg File .

### 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.

   You must use uppercase characters to provide the path of the script, for example,

   ```
   kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
   ```

   The installation or upgrade becomes completely automatic, without the need to specify the kickstart file during the installation or upgrade.

6 Recreate the ISO image:

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

#### Results

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.

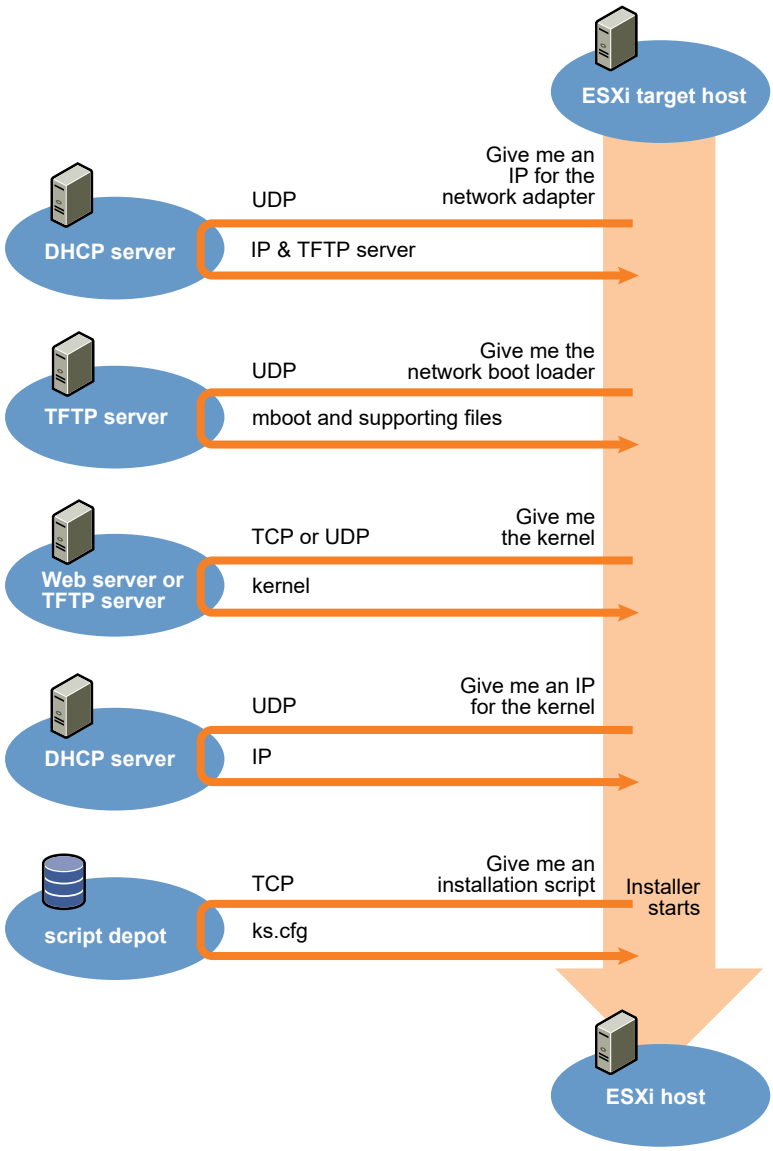
You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.

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 8-1. Overview of PXE Boot Installation Process



## Sample DHCP Configuration

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

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

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

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

### gPXE Example

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

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

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

### PXELINUX (without gPXE) Example

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

```
#
# DHCP Server Configuration file.
```

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

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

## About PXE Configuration Files

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

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

### Required Files

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

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

See About the boot.cfg File

### 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 and About the boot.cfg File .

### 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.
- DHCP server configured for PXE booting. See Sample DHCP Configuration.
- 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.
- 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 and About the boot.cfg File

### 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.

- DHCP server configured for PXE booting. See Sample DHCP Configuration.
- 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.
- 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 and About the boot.cfg File

### 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.
- 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.

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. 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.

# Download the ESXi Installer

Download the installer for ESXi.

### Prerequisites

Create a Customer Connect 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.

# Upgrading Hosts

9

After you upgrade vCenter Server and vSphere Update Manager, upgrade VMware ESXi 5.x hosts to ESXi 6.0. You can upgrade ESXi 5.0.x, ESXi 5.1.x, and ESXi 5.5.x hosts directly to ESXi 6.0.

To upgrade hosts, you can use the tools and methods that are described in Upgrade Options for ESXi 6.0.

**Caution** If you upgrade hosts managed by vCenter Server, you must upgrade to vCenter Server before you upgrade ESXi. If you do not upgrade in the correct order, you can lose data and lose access to servers.

This chapter includes the following topics:

- Using vSphere Update Manager to Perform Orchestrated Host Upgrades
- Installing or Upgrading Hosts by Using a Script
- Using vSphere Auto Deploy to Reprovision Hosts
- Upgrading Hosts by Using esxcli Commands
- Upgrade Hosts Interactively

## Using vSphere Update Manager to Perform Orchestrated Host Upgrades

Orchestrated upgrades allow you to upgrade the objects in your vSphere inventory in a two-step process: host upgrades, followed by virtual machine upgrades. You can configure the process at the cluster level to automate more of the process, or you can configure it at the individual host or virtual machine level for granular control.

For example, you can define a host upgrade baseline to upgrade an ESXi 5.x host to ESXi 6.0, or you can define a virtual machine upgrade baseline to upgrade the VMware Tools and the virtual machine hardware to the latest version. Use wizard-based workflows to first schedule host upgrades for an entire cluster and then schedule a virtual machine upgrade for all the virtual machines.

**Important** After you upgrade your host to ESXi 6.0, you cannot roll back to your version 5.x ESXi software. Back up your host before you perform an upgrade, so that, if the upgrade or migration fails, you can restore your 5.x host.

The wizard workflows prevent erroneous upgrade sequences. For example, the wizard prevents you from upgrading virtual machine hardware before you upgrade hosts in a cluster.

You can use Distributed Resource Scheduler (DRS) to prevent virtual machine downtime during the upgrade process.

Update Manager monitors hosts and virtual machines for compliance against your defined upgrade baselines. Noncompliance appears in detailed reports and in the dashboard view. Update Manager supports mass remediation.

The following vSphere components are upgraded by Update Manager.

- ESXi kernel (vmkernel)
- Virtual machine hardware
- VMware Tools
- Virtual appliances

For components that are not listed here, you can perform the upgrade by using another upgrade method, or, for third-party components, by using the appropriate third-party tools.

The following topics describe how to use Update Manager to conduct an orchestrated upgrade of your ESXi hosts.

- Configuring Host and Cluster Settings
- Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager

To use Update Manager to conduct an orchestrated upgrade of virtual machines on your hosts, see the *Installing and Administering VMware vSphere Update Manager* documentation.

## Configuring Host and Cluster Settings

When you update vSphere objects in a cluster with vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), and vSphere Fault Tolerance (FT) enabled, you can temporarily disable vSphere Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update completes, Update Manager restores these features.

Updates might require the host to enter maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, vCenter Server can migrate virtual machines to other ESXi hosts within a cluster before the host is put into maintenance mode. vCenter Server migrates the virtual machines if the cluster is configured for vSphere vMotion, and if DRS is enabled.

If a host has no running virtual machines, DPM might put the host in standby mode and interrupt an Update Manager operation. To make sure that scanning and staging complete successfully, Update Manager disables DPM during these operations. To ensure successful remediation, have Update Manager disable DPM and HA admission control before the remediation operation. After the operation completes, Update Manager restores DPM and HA admission control. Update Manager disables HA admission control before staging and remediation but not before scanning.

If DPM has already put hosts in standby mode, Update Manager powers on the hosts before scanning, staging, and remediation. After the scanning, staging, or remediation is complete, Update Manager turns on DPM and HA admission control and lets DPM put hosts into standby mode, if needed. Update Manager does not remediate powered off hosts.

If hosts are put into standby mode and DPM is manually disabled for a reason, Update Manager does not remediate or power on the hosts.

Within a cluster, temporarily disable HA admission control to allow vSphere vMotion to proceed. This action prevents downtime of the machines on the hosts that you remediate. After the remediation of the entire cluster, Update Manager restores HA admission control settings.

If FT is turned on for any of the virtual machines on hosts within a cluster, temporarily turn off FT before performing any Update Manager operations on the cluster. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. Remediate all hosts in a cluster with the same updates, so that FT can be reenabled after the remediation. A primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESXi version and patch levels.

As you remediate hosts that are part of a Virtual SAN cluster, be aware of the following behavior:

- The host remediation process might take an extensive amount of time to complete.
- By design, only one host from a Virtual SAN cluster can be in a maintenance mode at any time.
- Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you set the option to remediate the hosts in parallel.
- If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can workaround this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

## Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager

You can use vSphere Update Manager to perform orchestrated upgrades of the ESXi hosts in your vSphere inventory by using a single upgrade baseline, or by using a baseline group.

This workflow describes the overall process to perform an orchestrated upgrade of the hosts in your vSphere inventory. vSphere Update Manager 6.0 supports host upgrades to ESXi 6.0 for hosts that are running ESXi 5.x.

You can perform orchestrated upgrades of hosts at the folder, cluster, or data center level.

**Note** The last two steps in this procedure are alternatives. Choose one or the other.

### Prerequisites

- Make sure your system meets the requirements for vCenter Server 6.0, ESXi 6.0, and vSphere Update Manager 6.0. See Upgrade the Update Manager Server
- Install or upgrade vCenter Server to version 6.0. See Chapter 4 Upgrading and Updating vCenter Server for Windows.
- Install or upgrade vSphere Update Manager to version 6.0. See Chapter 7 Upgrading Update Manager.

### Procedure

1 Configure Host Maintenance Mode Settings

ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

2 Configure Cluster Settings

For ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

3 Enable Remediation of PXE Booted ESXi Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

4 Import Host Upgrade Images and Create Host Upgrade Baselines

You can create upgrade baselines for ESXi hosts with ESXi 6.0 images that you import to the Update Manager repository.

5 Create a Host Baseline Group

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

6 Attach Baselines and Baseline Groups to Objects

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

7 Manually Initiate a Scan of ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

8 View Compliance Information for vSphere Objects

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

9 Remediate Hosts Against an Upgrade Baseline

You can remediate ESXi hosts against a single attached upgrade baseline at a time. You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 6.0 image.

10 Remediate Hosts Against Baseline Groups

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

## Configure Host Maintenance Mode Settings

ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

For hosts in a container different from a cluster or for individual hosts, migration of the virtual machines with vMotion cannot be performed. If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

Hosts that are part of a Virtual SAN cluster can enter maintenance mode only one at a time. This is specificity of the Virtual SAN clusters.

If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can workaround this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

### Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

2 Depending on the client you use to connect to vCenter Server perform the following steps.

| Client | Steps |
|---|---|
| vSphere Web Client | 1 On the **Settings** tab, under Manage, click **Host/ Cluster Settings**.<br>Click **Edit**. |
| vSphere Client | 1 On the **Configuration** tab, under Settings, click **ESXi Host/Cluster Settings**. |

3 Under Maintenance Mode Settings, select an option from the **VM Power state** drop-down menu to determine the change of the power state of the virtual machines and appliances that are running on the host to be remediated.

| Option | Description |
|---|---|
| **Power Off virtual machines** | Powers off all virtual machines and virtual appliances before remediation. |
| **Suspend virtual machines** | Suspends all running virtual machines and virtual appliances before remediation. |
| **Do Not Change VM Power State** | Leaves virtual machines and virtual appliances in their current power state. This is the default setting. |

4 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the retry delay, and the number of retries.

If a host fails to enter maintenance mode before remediation, Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

5 (Optional) Select **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode**.

Update Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation.

After remediation, Update Manager reconnects the removable media devices if they are still available.

6 Click **Apply**.

Results

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

## Configure Cluster Settings

For ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control,

or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

**Note** Remediating hosts in parallel can improve performance significantly by reducing the time required for cluster remediation. Update Manager remediates hosts in parallel without disrupting the cluster resource constraints set by DRS. Avoid remediating hosts in parallel if the hosts are part of a Virtual SAN cluster. Due to the specifics of the Virtual SAN cluster, a host cannot enter maintenance mode while other hosts in the cluster are currently in maintenance mode.

### Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

2 Depending on the client you use to connect to vCenter Server perform the following steps.

| Client | Steps |
|---|---|
| vSphere Web Client | 1 On the **Manage** tab, under Settings, click **Host/ Cluster Settings**.<br>2 Click **Edit**. |
| vSphere Client | 1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**. |

3 Select the check boxes for features that you want to disable or enable.

| Option | Description |
|---|---|
| **Distributed Power Management (DPM)** | VMware DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state.<br>If you do not choose to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you choose to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates the hosts in the cluster, and re-enables VMware DPM after remediation is complete. |
| **High Availability (HA) admission control** | Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.<br>If you do not choose to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you choose to temporarily disable HA admission control, Update Manager disables HA admission control, remediates the cluster, and re-enables HA admission control after remediation is complete. |

| Option | Description |
| --- | --- |
| **Fault Tolerance (FT)** | FT provides continuous availability for virtual machines by automatically creating and maintaining a secondary virtual machine that is identical to the primary virtual machine. If you do not choose to turn off FT for the virtual machines on a host, Update Manager does not remediate that host. |
| **Enable parallel remediation for hosts in cluster** | Update Manager can remediate hosts in clusters in a parallel manner. Update Manager continuously evaluates the maximum number of hosts it can remediate in parallel without disrupting DRS settings. If you do not select the option, Update Manager remediates the hosts in a cluster sequentially.<br>By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. |
| **Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode** | Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can select to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane. |

4 Click **Apply**.

### Results

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

## Enable Remediation of PXE Booted ESXi Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

The global setting in the Update Manager **Configuration** tab enables solutions such as ESX Agent Manager or Cisco Nexus 1000V to initiate remediation of PXE booted ESXi hosts. In contrast, the **Enable patch remediation of powered on PXE booted ESXi hosts** setting in the **Remediate** wizard enables Update Manager to patch PXE booted hosts.

To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with Update Manager, so that the updates are not lost because of a reboot. Update Manager itself does not reboot the hosts because it does not install updates requiring a reboot on PXE booted ESXi hosts.

### Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

2 Depending on the client you use to connect to vCenter Server perform the following steps.

| Client | Steps |
|---|---|
| vSphere Web Client | 1 On the **Manage** tab, under Settings, click **Host/ Cluster Settings**.<br>2 Click **Edit**. |
| vSphere Client | 1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**. |

3 To enable installation of software for solutions on PXE booted ESXi hosts, select **Allow installation of additional software on PXE booted ESXi hosts.**

4 Click **Apply**.

## Import Host Upgrade Images and Create Host Upgrade Baselines

You can create upgrade baselines for ESXi hosts with ESXi 6.0 images that you import to the Update Manager repository.

You can use ESXi `.iso` images to upgrade ESXi 5.x hosts to ESXi 6.0.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

### Prerequisites

Ensure that you have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications icon.

### Procedure

1 On the **ESXi Images** tab click **Import ESXi Image** on the upper-right side.

2 On the Select ESXi Image page of the **Import ESXi Image** wizard, browse to and select the ESXi image that you want to upload.

3 Click **Next**.

**Caution** Do not close the import wizard. Closing the import wizard stops the upload process.

4 (Optional) In the **Security Warning** window, select an option to handle the certificate warning.

A trusted certificate authority does not sign the certificates that are generated for vCenter Server and ESXi hosts during installation. Because of this, each time an SSL connection is made to one of these systems, the client displays a warning.

| Option | Action |
|---|---|
| **Ignore** | Click **Ignore** to continue using the current SSL certificate and start the upload process. |
| **Cancel** | Click **Cancel** to close the window and stop the upload process. |
| **Install this certificate and do not display any security warnings** | Select this check box and click **Ignore** to install the certificate and stop receiving security warnings. |

5 After the file is uploaded, click **Next**.

6 (Optional) Create a host upgrade baseline.

a Leave the **Create a baseline using the ESXi image** selected.

b Specify a name, and optionally, a description for the host upgrade baseline.

7 Click **Finish**.

#### Results

The ESXi image that you uploaded appears in the Imported ESXi Images pane. You can see more information about the software packages that are included in the ESXi image in the Software Packages pane.

If you also created a host upgrade baseline, the new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

#### What to do next

To upgrade the hosts in your environment, you must create a host upgrade baseline if you have not already done so.

## Create a Host Baseline Group

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

**Note** You can click **Finish** in the **New Baseline Group** wizard at any time to save your baseline group and add baselines to it at a later stage.

#### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

2 On the **Baselines and Groups** tab, click **Create** above the Baseline Groups pane.

3 Depending on the client you use to connect to vCenter Server perform the following steps.

| Client | Steps |
| --- | --- |
| vSphere Web Client | 1 On the **Host Baselines** tab under **Manage**, click the **Create** above the Baseline Groups pane.<br>2 Enter a unique name for the baseline group and click **Next**. |
| vSphere Client | 1 On the **Baselines and Groups** tab, click the **Create** above the Baseline Groups pane.<br>2 Enter a unique name for the baseline group<br>3 Under Baseline Group Type, select **Host Baseline Group** and click **Next**. |

4 Select a host upgrade baseline to include it in the baseline group.

5 (Optional) If you use the vSphere Client create a new host upgrade baseline by clicking **Create a new Host Upgrade Baseline** at the bottom of the Upgrades page and complete the **New Baseline** wizard.

6 Click **Next**.

7 Select the patch baselines that you want to include in the baseline group.

8 (Optional) If you use the vSphere Client, create a new patch baseline by clicking **Create a new Host Patch Baseline** at the bottom of the Patches page and complete the **New Baseline** wizard.

9 Click **Next**.

10 Select the extension baselines to include in the baseline group.

11 (Optional) If you use the vSphere Client, create a new extension baseline by clicking **Create a new Extension Baseline** at the bottom of the Patches page and complete the **New Baseline** wizard.

12 On the Ready to Complete page, click **Finish**.

#### Results

The host baseline group is displayed in the Baseline Groups pane.

## Attach Baselines and Baseline Groups to Objects

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

You can attach baselines and baseline groups to objects from the Update Manager Client Compliance view.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and data centers. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can attach baselines and baseline groups to objects managed by the vCenter Server system with which Update Manager is registered. Baselines and baseline groups you attach are specific for the Update Manager instance that is registered with the vCenter Server system.

#### Prerequisites

Ensure that you have the **Attach Baseline** privilege.

#### Procedure

1. Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Inventory**.
2. Select the type of object that you want to attach the baseline to.

   For example, **Hosts and Clusters** or **VMs and Templates**.
3. Select the object in the inventory, and click the **Update Manager** tab.

   If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, the **Update Manager** tab is available only for the vCenter Server system with which an Update Manager instance is registered.
4. Click **Attach** in the upper-right corner.
5. In the **Attach Baseline or Group** window, select one or more baselines or baseline groups to attach to the object.

   If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.
6. (Optional) Click the **Create Baseline Group** or **Create Baseline** links to create a baseline group or a baseline and complete the remaining steps in the respective wizard.
7. Click **Attach**.

#### Results

The baselines and baseline groups that you selected to attach are displayed in the Attached Baseline Groups and Attached Baselines panes of the **Update Manager** tab.

## Manually Initiate a Scan of ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

#### Procedure

1. Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.
2. Right-click a host, data center, or any container object and select **Scan for Updates**.

3 Select the types of updates to scan for.

You can scan for either **Patches and Extensions** or **Upgrades**.

4 Click **Scan**.

### Results

The selected inventory object and all child objects are scanned against all patches, extensions, and upgrades in the attached baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

## View Compliance Information for vSphere Objects

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

When you select a container object, you view the overall compliance status of the attached baselines, as well as all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

2 Select the type of object for which you want to view compliance information.

| Client | Steps |
|---|---|
| vSphere Web Client | 1 Depending on the compliance information you want to see, perform the following steps:<br>a To view host compliance information, select **Home > Hosts and Clusters**, and select a host, a cluster, a datacenter or a vCenter Server instance.<br>b To view virtual machine compliance information, select **Home > VMs and Templates**, and select a virtual machine, a folder or a virtual appliance.<br>2 Select **Manage** tab, and then select **Update Manager** tab. |
| vSphere Client | 1 Depending on the compliance information you want to see, perform the following steps:<br>a To view host compliance information, select **Home > Inventory > Hosts and Clusters**, and select a host, a cluster, a datacenter or a vCenter Server instance.<br>b To view virtual machine compliance information, select **Home > Inventory > VMs and Templates**, and select a virtual machine, a folder or a virtual appliance.<br>2 Select the **Update Manager** tab. |

3 Select one of the attached baselines to view compliance information for the object against that baseline.

## Remediate Hosts Against an Upgrade Baseline

You can remediate ESXi hosts against a single attached upgrade baseline at a time. You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 6.0 image.

**Note** Alternatively, you can upgrade hosts by using a baseline group. See Remediate Hosts Against Baseline Groups.

Update Manager 6.0 supports upgrade from ESXi 5.x to ESXi 6.0. Host upgrades to ESXi 5.0, ESXi 5.1 or ESXi 5.5 are not supported.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.0.0-build_number.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Any third-party software modules on a ESXi 5.x host will remain intact after upgrade to ESXi 6.0.

**Note** In case of an unsuccessful upgrade from ESXi 5.x to ESXi 6.0, you cannot roll back to your previous ESXi 5.x instance.

### Prerequisites

To remediate a host against an upgrade baseline, attach the baseline to the host.

Review any scan messages in the **Upgrade Details** window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade to ESXi 6.0.

### Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

| Client | Steps |
|---|---|
| vSphere Web Client | 1 Select **Home > Hosts and Clusters**.<br>2 From the inventory object navigator, right-click a datacenter, a cluster, or a host, and select **Update Manager > Remediate**.<br>If you select a container object, all hosts under the selected object are remediated. |
| vSphere Client | 1 Select **Home > Inventory > Hosts and Clusters**, in the navigation bar.<br>2 From the object navigator, right-click a datacenter, a cluster, or a host, and select **Remediate**.<br>If you select a container object, all hosts under the selected object are remediated. |

The Remediate wizard opens.

2 Select **Upgrade Baselines**.

3 On the Remediation Selection page of the Remediate wizard, select the upgrade baseline to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESXi 6.0 Upgrade page, select the option to ignore warnings about unsupported devices on the host, or no longer supported VMFS datastore in order to continue with the remediation.

7 Click **Next**.

8 On the Schedule page, specify a unique name and an optional description for the task.

The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

9 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

10 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

| Option | Description |
|---|---|
| **Power Off virtual machines** | Power off all virtual machines and virtual appliances before remediation. |
| **Suspend virtual machines** | Suspend all running virtual machines and virtual appliances before remediation. |
| **Do Not Change VM Power State** | Leave virtual machines and virtual appliances in their current power state.<br>A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster. |

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

11 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

12 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

13 Click **Next**.

14 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

| Option | Details |
|---|---|
| **Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.** | Update Manager does not remediate clusters with active DPM.<br>DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation. |
| **Disable High Availability admission control if it is enabled for any of the selected clusters.** | Update Manager does not remediate clusters with active HA admission control.<br>Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. |
| **Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.** | If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host.<br>For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled. |

| Option | Details |
| --- | --- |
| **Enable parallel remediation for the hosts in the selected clusters.** | Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially.<br>By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.<br>By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.<br>**Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page. |
| **Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.** | Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane. |

15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

16 On the Ready to Complete page, click **Finish**.

Example

**Note** In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

## Remediate Hosts Against Baseline Groups

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

You can perform an orchestrated upgrade by using a host baseline group. The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

**Note** Alternatively, you can upgrade hosts by using a single upgrade baseline. See Remediate Hosts Against an Upgrade Baseline.

### Prerequisites

Ensure that at least one baseline group is attached to the host.

Review any scan messages in the **Upgrade Details** window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade to ESXi 6.0.

Procedure

1 Use the vSphere Client or the vSphere Web Client to connect to a vCenter Server system with which Update Manager is registered.

| Client | Steps |
| --- | --- |
| vSphere Web Client | 1 Select **Home > Hosts and Clusters**.<br>2 From the inventory object navigator, right-click a datacenter, a cluster, or a host, and select **Update Manager > Remediate**.<br>If you select a container object, all hosts under the selected object are remediated. |
| vSphere Client | 1 Select **Home > Inventory > Hosts and Clusters**, in the navigation bar.<br>2 From the object navigator, right-click a datacenter, a cluster, or a host, and select **Remediate**. If you select a container object, all hosts under the selected object are remediated.<br>If you select a container object, all hosts under the selected object are remediated. |

The Remediate wizard opens.

2 On the Remediation Selection page of the **Remediate** wizard, select the baseline group and baselines to apply.

3 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

4 On the End User License Agreement page, accept the terms and click **Next**.

5 (Optional) On the ESXi 6.0 Upgrade page, select the option to ignore warnings about unsupported devices on the host, or no longer supported VMFS datastore in order to continue with the remediation.

6 Click **Next**.

7 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process, and click **Next**.

8 (Optional) On the Dynamic Patches and Extensions to Exclude page, review the list of patches or extensions to be excluded and click **Next**.

9 On the Schedule page, specify a unique name and an optional description for the task.

The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

10 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

11 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

| Option | Description |
|---|---|
| **Power Off virtual machines** | Power off all virtual machines and virtual appliances before remediation. |
| **Suspend virtual machines** | Suspend all running virtual machines and virtual appliances before remediation. |
| **Do Not Change VM Power State** | Leave virtual machines and virtual appliances in their current power state.<br>A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster. |

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

12 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

13 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

14 (Optional) Select the check box under ESXi Patch Settings to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

15 Click **Next**.

16 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

| Option | Details |
|---|---|
| **Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.** | Update Manager does not remediate clusters with active DPM.<br>DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation. |
| **Disable High Availability admission control if it is enabled for any of the selected clusters.** | Update Manager does not remediate clusters with active HA admission control.<br>Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. |
| **Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.** | If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host.<br>For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled. |
| **Enable parallel remediation for the hosts in the selected clusters.** | Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially.<br>By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.<br>By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.<br>**Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page. |
| **Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.** | Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane. |

17 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

18 On the Ready to Complete page, click **Finish**.

Example

**Note** In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

# 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

## 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 and PXE Booting the ESXi Installer.

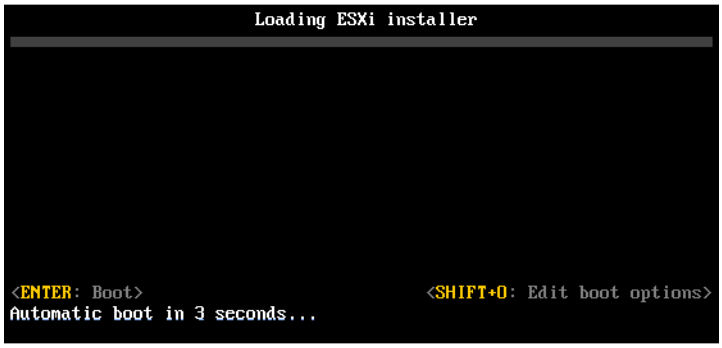
To specify the location of the installation script, set the `ks=`*`filepath`* option, where *filepath* is indicates the location of your Kickstart file. Otherwise, a scripted installation or upgrade cannot start. If `ks=`*`filepath`* is omitted, the text installer is run.

Supported boot options are listed in Boot Options .

Procedure

1 Start the host.

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




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

### Example: Boot Option

You type the following boot options:

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

## Boot Options

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

### Supported Boot Options

**Table 9-1. 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. |

Table 9-1. Boot Options for ESXi Installation (continued)

| Boot Option | Description |
| --- | --- |
| `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.<br>**Important** If you have created an installer ISO image with a custom installation or upgrade script, you must use uppercase characters to provide the path of the script, for example, `ks=cdrom:/KS_CUST.CFG`. |
| `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.

## 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.
- USB Flash drive. See Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script.
- 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.

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.

## 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.

**--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.

**`--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.<br>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:<br>■ Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*<br>■ MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*<br>■ VML name: `--disk=`*`vml.000000034211234`*<br>■ vmkLUN UID:`--disk=`*`vmkLUN_UID`*<br>For accepted disk name formats, see Disk Device Names. |
| **`--firstdisk=`**<br>***`disk-type1,`***<br>**`[`*****`disk-type2`*****`,...]`** | Partitions the first eligible disk found. By default, the eligible disks are set to the following order:<br>1 Locally attached storage (`local`)<br>2 Network storage (`remote`)<br>3 USB disks (`usb`)<br>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 =[python\|busybox]** | Specifies an interpreter to use. The default is busybox. |

### %post (optional)

Runs the specified script after package installation is complete. If you specify multiple `%post` sections, they run in the order that they appear in the installation script.

| | |
|---|---|
| **--interpreter =[python\|busybox]** | Specifies an interpreter to use. The default is busybox. |
| **--timeout=secs** | Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully terminated. |
| **--ignorefailure =[true\|false]** | If true, the installation is considered a success even if the `%post` script terminated with an error. |

### %firstboot

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

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

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

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

## Disk Device Names

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

Table 9-2. 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 9-3. 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 (---). |

For example, to modify the `boot.cfg` file with information for an HTTP server, see PXE Boot the ESXi Installer Using gPXE.

See also Create an Installer ISO Image with a Custom Installation or Upgrade Script, PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File, PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File, and PXE Booting the ESXi Installer.

# 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.

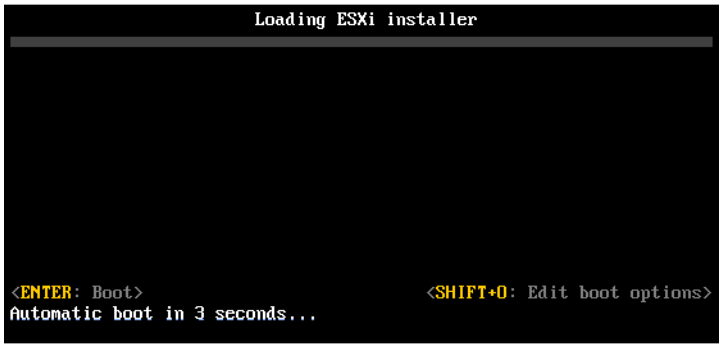
### Prerequisites

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.
- 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.
- 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.
- You have selected a boot command to run the scripted installation or upgrade. See Enter Boot Options to Start an Installation or Upgrade Script. For a complete list of boot commands, see Boot Options .

### 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.




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.

### Results

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 .

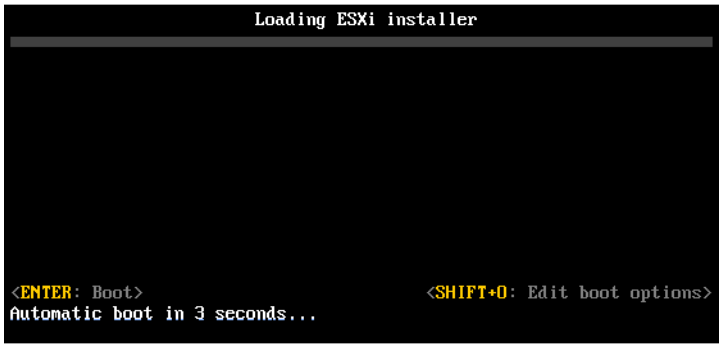
### Prerequisites

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.
- 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.
- 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.
- 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.

### Procedure

1. Boot the ESXi installer from the USB flash drive.
2. When the ESXi installer window appears, press Shift+O to edit boot options.




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

   The boot option has the form `ks=`.
4. Press Enter.

### Results

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.
- For information about creating and locating an installation script, see About Installation and Upgrade Scripts.
- 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
  - PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File
  - PXE Boot the ESXi Installer Using gPXE
- For information about using vSphere Auto Deploy to perform a scripted upgrade by using PXE to boot, see Using vSphere Auto Deploy to Reprovision Hosts .

# Using vSphere Auto Deploy to Reprovision Hosts

If a host was deployed using vSphere Auto Deploy, you can use Auto Deploy to reprovision the host with a new image profile that contains a different version of ESXi. You can use the ESXi Image Builder PowerCLI to create and manage image profiles.

**Note** If you upgrade the host to use an ESXi 6.0 or later image, the Auto Deploy server provisions the ESXi host with certificates that are signed by VMCA. If you are currently using custom certificates, you can set up the host to use the custom certificates after the upgrade.

The Auto Deploy server is automatically upgraded if you upgrade the corresponding vCenter Server system to version 6. Starting with version 6, the Auto Deploy server is always on the same management node as the vCenter Server system.

## 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 the topic "Preparing for vSphere Auto Deploy" in the *vSphere installation and Setup* documentation.

The following reprovisioning operations are available.

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

- Reprovision with a different host profile.

## Reprovision Hosts with Simple Reboot Operations

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

Setup includes DHCP server setup, writing rules, and making an image 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.

### Results

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 boot the host with. Use the Image Builder PowerCLI. See "Using vSphere ESXi Image Builder CLI" in the *vSphere Installation and Setup* documentation.
- Make sure that the setup that you performed during the first boot operation is in place.

### Procedure

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

   **`Connect-VIServer myVCServer`**

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

2. Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with the Image Builder PowerCLI.
3. Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

| Depot Type | Cmdlet |
|---|---|
| **Remote depot** | Run **`Add-EsxSoftwareDepot`** ***`depot_url`***. |
| **ZIP file** | a Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine.<br>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 .

### Results

When you reboot hosts after compliance repair, Auto Deploy provisions the hosts 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. For information see *vSphere Installation and Setup*.
- 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 .
- Power on unprovisioned hosts to provision them with the host profile.

## Test and Repair Rule Compliance

When you add a rule to the Auto Deploy rule set or make changes to one or more rules, hosts are not updated automatically. Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

### 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.

# Upgrading Hosts by Using esxcli Commands

By using vSphere CLI, you can upgrade ESXi 5.x host to version 6.0 and update or patch ESXi 5.x and 6.0 hosts.

To use esxcli commands for vCLI , you must install vSphere CLI (vCLI). For more information about installing and using the vCLI, see the following documents:

- *Getting Started with vSphere Command-Line Interfaces*
- *vSphere Command-Line Interface Concepts and Examples*
- *vSphere Command-Line Interface Reference* is a reference to `vicfg-` and related vCLI commands.

**Note** If you press Ctrl+C while an `esxcli` command is running, the command-line interface exits to a new prompt without displaying a message. However, the command continues to run to completion.

For ESXi hosts deployed with vSphere Auto Deploy, the tools VIB must be part of the base booting image used for the initial Auto Deploy installation. The tools VIB cannot be added separately later.

## VIBs, Image Profiles, and Software Depots

Upgrading ESXi with esxcli commands requires an understanding of VIBs, image profiles, and software depots.

The following technical terms are used throughout the vSphere documentation set in discussions of installation and upgrade tasks.

**VIB**

A VIB is an ESXi software package. VMware and its partners package solutions, drivers, CIM providers, and applications that extend the ESXi platform as VIBs. VIBs are available in software depots. You can use VIBs to create and customize ISO images or to upgrade ESXi hosts by installing VIBs asynchronously onto the hosts.

**Image Profile**

An image profile defines an ESXi image and consists of VIBs. An image profile always includes a base VIB, and might include more VIBs. You examine and define an image profile by using vSphere ESXi Image Builder.

**Software Depot**

A software depot is a collection of VIBs and image profiles. The software depot is a hierarchy of files and folders and can be available through an HTTP URL (online depot) or a ZIP file (offline depot). VMware and VMware partners make depots available. Companies with large VMware installations might create internal depots to provision ESXi hosts with vSphere Auto Deploy, or to export an ISO for ESXi installation.

## Understanding Acceptance Levels for VIBS and Hosts

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host.

The acceptance level applies to individual VIBs installed by using the `esxcli software vib install` and `esxcli software vib update` commands, to VIBs installed using vSphere Update Manager, and to VIBs in image profiles.

The acceptance level of all VIBs on a host must be at least as high as the host acceptance level. For example, if the host acceptance level is VMwareAccepted, you can install VIBs with acceptance levels of VMwareCertified and VMwareAccepted, but you cannot install VIBs with acceptance levels of PartnerSupported or CommunitySupported. To install a VIB with a less restrictive acceptance level than that of the host, you can change the acceptance level of the host by using the vSphere Web Client or by running `esxcli software acceptance` commands.

Setting host acceptance levels is a best practice that allows you to specify which VIBs can be installed on a host and used with an image profile, and the level of support you can expect for a VIB. For example, you would probably set a more restrictive acceptance level for hosts in a production environment than for hosts in a testing environment.

VMware supports the following acceptance levels.

**VMwareCertified**

The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only I/O Vendor Program (IOVP) program 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.

Table 9-4. VIB Acceptance Levels Required to Install on Hosts

| Host Acceptance Level | VMwareCertified VIB | VMwareAccepted VIB | PartnerSupported VIB | CommunitySupported VIB |
|---|---|---|---|---|
| VMwareCertified | x | | | |
| VMwareAccepted | x | x | | |
| PartnerSupported | x | x | x | |
| CommunitySupported | x | x | x | x |

## Match a Host Acceptance Level with an Update Acceptance Level

You can change the host acceptance level to match the acceptance level for a VIB or image profile that you want to install. The acceptance level of all VIBs on a host must be at least as high as the host acceptance level.

Use this procedure to determine the acceptance levels of the host and the VIB or image profile to install, and to change the acceptance level of the host, if necessary for the update.

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

1 Retrieve the acceptance level for the VIB or image profile.

| Option | Description |
|---|---|
| List information for all VIBs | **esxcli --server=*server_name* software sources vib list --depot=*depot_URL*** |
| List information for a specified VIB | **esxcli --server=*server_name* software sources vib list --viburl=*vib_URL*** |
| List information for all image profiles | **esxcli --server=*server_name* software sources profile list --depot=*depot_URL*** |
| List information for a specified image profile | **esxcli --server=*server_name* software sources profile get --depot=*depot_URL* --profile=*profile_name*** |

2 Retrieve the host acceptance level.

**esxcli --server=*server_name* software acceptance get**

3 (Optional) If the acceptance level of the VIB is more restrictive than the acceptance level of the host, change the acceptance level of the host.

**esxcli --server=*server_name* software acceptance set --level=*acceptance_level***

The *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

**Note** You can use the `--force` option for the `esxcli software vib` or `esxcli software profile` command to add a VIB or image profile with a lower acceptance level than the host. A warning will appear. Because your setup is no longer consistent, the warning is repeated when you install VIBs, remove VIBs, and perform certain other operations on the host.

## Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted

VIBs that you can install with live install do not require the host to be rebooted, but might require the host to be placed in maintenance mode. Other VIBs and profiles might require the host to be rebooted after the installation or update.

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

1 Check whether the VIB or image profile that you want to install requires the host to be placed in maintenance mode or to be rebooted after the installation or update.

Run one of the following commands.

| Option | Description |
|---|---|
| Check the VIB | `esxcli --server=server_name software sources vib get -v absolute_path_to_vib` |
| Check the VIBs in a depot | `esxcli --server=server_name software sources vib get --depot=depot_name` |
| Check the image profile in a depot | `esxcli --server=server_name software sources profile get --depot=depot_name` |

2 Review the return values.

The return values, which are read from the VIB metadata, indicate whether the host must be in maintenance mode before installing the VIB or image profile, and whether installing the VIB or profile requires the host to be rebooted.

**Note** vSphere Update Manager relies on the `esxupdate`/`esxcli` scan result to determine whether maintenance mode is required or not. When you install a VIB on a live system, if the value for `Live-Install-Allowed` is set to false, the installation result will instruct Update Manager to reboot the host. When you remove a VIB from a live system, if the value for `Live-Remove-Allowed` is set to false, the removal result will instruct Update Manager to reboot the host. In either case, during the reboot, Update Manager will automatically put the host into maintenance mode.

### What to do next

If necessary, place the host in maintenance mode. See Place a Host in Maintenance Mode. If a reboot is required, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster before the installation or update.

## Place a Host in Maintenance Mode

Some installation and update operations that use live install require the host to be in maintenance mode.

To determine whether an upgrade operation requires the host to be in maintenance mode, see Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted

**Note** If the host is a member of a Virtual SAN cluster, and any virtual machine object on the host uses the "Number of failures to tolerate=0" setting in its storage policy, the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to evacuate this object from the host for the maintenance operation to complete successfully.

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

1 Check whether the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

2 Power off each virtual machines running on the ESXi host.

| Option | Command |
|---|---|
| To shut down the guest operating system and then power off the virtual machine | `vmware-cmd --server=server_name path_to_vm stop soft` |
| To force the power off operation | `vmware-cmd --server=server_name path_to_vm stop hard` |

Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

3 Place the host in maintenance mode.

```
vicfg-hostops --server=server_name --operation enter
```

4 Verify that the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

# Update a Host with Individual VIBs

You can update a host with VIBs stored in a software depot that is accessible through a URL or in an offline ZIP depot.

**Important** If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic Upgrade or Update a Host with Image Profiles .

The **`esxcli software vib update`** and **`esxcli software vib install`** commands are not supported for upgrade operations. See Differences Between vSphere Upgrades and Updates and Upgrade or Update a Host with Image Profiles .

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted. See Place a Host in Maintenance Mode.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

### Procedure

1 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

2 Find out which VIBs are available in the depot.

| Option | Description |
|---|---|
| from a depot accessible by URL | `esxcli --server=server_name software sources vib list --depot=http://web_server/depot_name` |
| from a local depot ZIP file | `esxcli --server=server_name software sources vib list --depot=absolute_path_to_depot_zip_file` |

You can specify a proxy server by using the **`--proxy`** argument.

3 Update the existing VIBs to include the VIBs in the depot or install new VIBs.

| Option | Description |
|---|---|
| Update VIBs from a depot accessible by URL | `esxcli --server=server_name software vib update --depot=http://web_server/depot_name` |
| Update VIBs from a local depot ZIP file | `esxcli --server=server_name software vib update --depot=absolute_path_to_depot_ZIP_file` |
| Install all VIBs from a ZIP file on a specified offline depot (includes both VMware VIBs and partner-supplied VIBs) | `esxcli --server=server_name software vib install --depot path_to_VMware_vib_ZIP_file\VMware_vib_ZIP_file --depot path_to_partner_vib_ZIP_file\partner_vib_ZIP_file` |

Options for the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *esxcli Reference* at http://www.vmware.com/support/developer/vcli/.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

## Upgrade or Update a Host with Image Profiles

You can upgrade or update a host with image profiles stored in a software depot that is accessible through a URL or in an offline ZIP depot.

You can use the **`esxcli software profile update`** or **`esxcli software profile install`** command to upgrade or update an ESXi host. To understand the differences between upgrades and updates, see Differences Between vSphere Upgrades and Updates.

When you upgrade or update a host, the **`esxcli software profile update`** or **`esxcli software profile install`** command applies a higher version (major or minor) of a full image profile onto the host. After this operation and a reboot, the host can join to a vCenter Server environment of the same higher version.

The **`esxcli software profile update`** command brings the entire contents of the ESXi host image to the same level as the corresponding upgrade method using an ISO installer. However, the ISO installer performs a pre-upgrade check for potential problems, and the **`esxcli`** upgrade method does not. The ISO installer checks the host to make sure that it has sufficient memory for the upgrade, and does not have unsupported devices connected. For more about the ISO installer and other ESXi upgrade methods, see Upgrade Options for ESXi 6.0.

**Important** If you are upgrading or updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update command `esxcli software profile update --depot=depot_location --profile=profile_name`.

When you specify a target server by using **--server=server_name**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

**Note** Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted. See Place a Host in Maintenance Mode.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

1 Determine which VIBs are installed on the host.

  **esxcli --server=*server_name* software vib list**

2 Determine which image profiles are available in the depot.

  **esxcli --server=*server_name* software sources profile list --depot=http://*webserver/depot_name***

  You can specify a proxy server by using the **--proxy** argument.

3 Update the existing image profile to include the VIBs or install new VIBs.

**Important** The `software profile update` command updates existing VIBS with the corresponding VIBs from the specified profile, but does not affect other VIBs installed on the target server. The `software profile install` command installs the VIBs present in the depot image profile, and removes any other VIBS installed on the target server.

| Option | Description |
|---|---|
| Update the image profile from a VMware-supplied zip bundle, in a depot, accessible online from the VMware Web site or downloaded to a local depot. | **`esxcli software profile update --depot=`*`depot_location`*` --profile=`*`profile_name`**<br>**Important** This is the only update method that VMware supports for zip bundles supplied by VMware.<br>VMware-supplied zip bundle names take the form: **`VMware-ESXi-6.0.0-`*`build_number`*`-depot.zip`**<br>The profile name for VMware-supplied zip bundles takes one of the following forms.<br>■ **`ESXi-6.0.0-`*`build_number`*`-standard`**<br>■ **`ESXi-6.0.0-`*`build_number`*`-notools`** (does not include VMware Tools) |
| Update the image profile from a depot accessible by URL | **`esxcli --server=`*`server_name`*` software profile update --depot=http://`*`webserver/depot_name`*` --profile=`*`profile_name`** |
| Update the image profile from ZIP file stored locally on the target server | **`esxcli --server=`*`server_name`*` software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=`*`profile_name`** |
| Update the image profile from a ZIP file on the target server, copied into a datastore | **`esxcli --server=`*`server_name`*` software profile update --depot="[`*`datastore_name`*`]`*`profile_ZIP_file`*`" --profile=`*`profile_name`** |
| Update the image profile from a ZIP file copied locally and applied on the target server | **`esxcli --server=`*`server_name`*` software profile update --depot=/`*`root_dir/path_to_profile_ZIP_file/profile_ZIP_file`*` --profile=`*`profile_name`** |
| Install all new VIBs in a specified profile accessible by URL | **`esxcli --server=`*`server_name`*` software profile install --depot=http://`*`webserver/depot_name`*` --profile=`*`profile_name`** |
| Install all new VIBs in a specified profile from a ZIP file stored locally on the target | **`esxcli --server=`*`server_name`*` software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=`*`profile_name`** |
| Install all new VIBs from a ZIP file on the target server, copied into a datastore | **`esxcli --server=`*`server_name`*` software profile install --depot="[`*`datastore_name`*`]`*`profile_ZIP_file`*`" --profile=`*`profile_name`** |
| Install all new VIBs from a ZIP file copied locally and applied on the target server | **`esxcli --server=`*`server_name`*` software profile install --depot=/`*`root_dir/path_to_profile_ZIP_file/profile_ZIP_file`*` --profile=`*`profile_name`** |

**Note** Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

## Update ESXi Hosts by Using Zip Files

You can update hosts with VIBs or image profiles by downloading a ZIP file of a depot.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

**Important** If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic Upgrade or Update a Host with Image Profiles .

The **`esxcli software vib update`** and **`esxcli software vib install`** commands are not supported for upgrade operations. See Differences Between vSphere Upgrades and Updates and Upgrade or Update a Host with Image Profiles .

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Download the ZIP file of a depot bundle from a third-party VMware partner.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted. See Place a Host in Maintenance Mode.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

### Procedure

- Install the ZIP file.

  ```
  esxcli --server=server_name software vib update --depot=/path_to_vib_ZIP/ZIP_file_name.zip
  ```

## Remove VIBs from a Host

You can uninstall third-party VIBs or VMware VIBs from your ESXi host.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Prerequisites

- If the removal requires a reboot, and if the host belongs to a VMware HA cluster, disable HA for the host.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted. See Place a Host in Maintenance Mode.
- 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 Power off each virtual machines running on the ESXi host.

| Option | Command |
|---|---|
| To shut down the guest operating system and then power off the virtual machine | **vmware-cmd --server=*server_name path_to_vm* stop soft** |
| To force the power off operation | **vmware-cmd --server=*server_name path_to_vm* stop hard** |

  Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

2 Place the host in maintenance mode.

  **vicfg-hostops --server=*server_name* --operation enter**

3 If necessary, shut down or migrate virtual machines.

4 Determine which VIBs are installed on the host.

  **esxcli --server=*server_name* software vib list**

5 Remove the VIB.

  **esxcli --server=*server_name* software vib remove --vibname=*name***

  Specify one or more VIBs to remove in one of the following forms:

  - ***name***

- ***name*:*version***
- ***vendor*:*name***
- ***vendor*:*name*:*version***

For example, the command to remove a VIB specified by vendor, name and version would take this form:

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

**Note** The `remove` command supports several more options. See the *vSphere Command-Line Interface Reference*.

## Adding Third-Party Extensions to Hosts with an esxcli Command

You can use the `esxcli software vib` command to add to the system a third-party extension released as a VIB package. When you use this command, the VIB system updates the firewall rule set and refreshes the host daemon after you reboot the system.

Otherwise, you can use a firewall configuration file to specify port rules for host services to enable for the extension. The *vSphere Security* documentation discusses how to add, apply, and refresh a firewall rule set and lists the `esxcli network firewall` commands.

## Perform a Dry Run of an esxcli Installation or Upgrade

You can use the `--dry-run` option to preview the results of an installation or upgrade operation. A dry run of the installation or update procedure does not make any changes, but reports the VIB-level operations that will be performed if you run the command without the `--dry-run` option.

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

1 Enter the installation or upgrade command, adding the **--dry-run** option.

- **`esxcli --server=server_name software vib install --dry-run`**
- **`esxcli --server=server_name software vib update --dry-run`**

- **esxcli --server=*server_name* software profile install --dry-run**
- **esxcli --server=*server_name* software profile update --dry-run**

2 Review the output that is returned.

The output shows which VIBs will be installed or removed and whether the installation or update requires a reboot.

## Display the Installed VIBs and Profiles That Will Be Active After the Next Host Reboot

You can use the `--rebooting-image` option to list the VIBs and profiles that are installed on the host and will be active after the next host reboot.

When you specify a target server by using **--server=server_name**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

1 Enter one of the following commands.

| Option | Description |
|---|---|
| For VIBs | **esxcli --server=*server_name* software vib list --rebooting-image** |
| For Profiles | **esxcli --server=*server_name* software profile get --rebooting-image** |

2 Review the output that is returned.

The output displays information for the ESXi image that will become active after the next reboot. If the pending-reboot image has not been created, the output returns nothing.

## Display the Image Profile and Acceptance Level of the Host

You can use the `software profile get` command to display the currently installed image profile and acceptance level for the specified host.

This command also shows details of the installed image profile history, including profile modifications.

When you specify a target server by using **`--server=server_name`**, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

#### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

#### Procedure

1 Enter the following command.

```
esxcli --server=server_name software profile get
```

2 Review the output.

## Upgrade Hosts Interactively

To upgrade ESXi 5.x hosts to ESXi 6.0, you can boot the ESXi installer from a CD, DVD, or USB flash drive.

Before upgrading, consider disconnecting the network storage. This action decreases the time it takes the installer to search for available disk drives. When you disconnect network storage, any files on the disconnected disks are unavailable at installation. Do not disconnect a LUN that contains an existing ESXi installation.

#### Prerequisites

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

  **Note** You can also use PXE to boot the ESXi installer to run an interactive installation or a scripted installation. See PXE Booting the ESXi Installer.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- ESXi Embedded must not be on the host. ESXi Installable and ESXi Embedded cannot exist on the same host.
- If you are upgrading a 5.0.x or 5.1.x host, supported custom VIBs that are not included in the ESXi installer ISO are migrated. See Upgrading Hosts That Have Third-Party Custom VIBs
- See your hardware vendor documentation for information about changing the boot order.

Procedure

1 Insert the ESXi installer CD or DVD in the CD-ROM or 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.

3 In the Select a Disk panel, select the drive on which to install or upgrade ESXi and press Enter.

Press F1 for information about the selected disk.

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

4 Upgrade or install ESXi if the installer finds an existing ESXi installation and VMFS datastore.

If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

5 Press F11 to confirm and start the upgrade.

6 Remove the installation CD or DVD or USB flash drive when the upgrade is complete.

7 Press Enter to reboot the host.

8 Set the first boot device to be the drive which you selected previously when you upgraded ESXi.

# After You Upgrade ESXi Hosts

10

To complete a host upgrade, you ensure that the host is reconnected to its managing vCenter Server system and reconfigured if necessary. You also check that the host is licensed correctly.

After you upgrade an ESXi host, take the following actions:

- View the upgrade logs. You can use the vSphere Web Client to export the log files.
- If a vCenter Server system manages the host, you must reconnect the host to vCenter Server by right-clicking the host in the vCenter Server inventory and selecting **Connect**.
- When the upgrade is complete, the ESXi host is in evaluation mode. The evaluation period is 60 days. You must assign a vSphere 6.0 license before the evaluation period expires. You can upgrade existing licenses or acquire new ones from Customer Connect. Use the vSphere Web Client to configure the licensing for the hosts in your environment. See the *vCenter Server and Host Management* documentation for details about managing licenses in vSphere.
- The host sdX devices might be renumbered after the upgrade. If necessary, update any scripts that reference sdX devices.
- Upgrade virtual machines on the host. See Chapter 11 Upgrading Virtual Machines and VMware Tools.

This chapter includes the following topics:



## 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.

## Applying Licenses After Upgrading to ESXi 6.0

After you upgrade to ESXi 6.0, you must apply a vSphere 6.0 license.

When you upgrade ESXi 5.x hosts to ESXi 6.0 hosts, the hosts are in a 60-day evaluation mode period until you apply the correct vSphere 6.0 licenses. See About ESXi Evaluation and Licensed Modes.

You can upgrade your existing vSphere 5.x licenses or acquire vSphere 6.0 licenses from Customer Connect. After you have vSphere 6.0 licenses, you must assign them to all upgraded ESXi 6.0 hosts by using the license management functionality in the vSphere Web Client. See the *vCenter Server and Host Management* documentation for details. If you use the scripted method to upgrade to ESXi 6.0, you can provide the license key in the kickstart (ks) file.

## 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 10-1. 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 and configuring syslog and a syslog server and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

# 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. |

| Option | Description |
| --- | --- |
| **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**.

### Results

Changes to the syslog options take effect immediately.

# Upgrading Virtual Machines and VMware Tools

11

After you upgrade ESXi hosts, you can upgrade the virtual machines on the host to take advantage of new features.

VMware offers the following tools for upgrading virtual machines:

**vSphere Web Client**

Requires you to perform the virtual machine upgrade one step at a time, but does not require vSphere Update Manager. See the information about upgrading virtual machines in the *vSphere Virtual Machine Administration* documentation.

**vSphere Update Manager**

Automates the process of upgrading and patching virtual machines, thereby ensuring that the steps occur in the correct order. You can use Update Manager to directly upgrade the virtual machine hardware version and VMware Tools. See the *Installing and Administering VMware vSphere Update Manager* documentation.

# Troubleshooting a vSphere Upgrade

12

The installation and upgrade software enables you to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log file. You can also consult the product release notes for known problems.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

The *vSphere Ugrade* guide describes how to use VMware products and their features. If you encounter problems or error situations that are not described in this guide, you may find a solution in VMware Knowledge Base. You can also use VMware Community Forums to find others with same problem or ask for help, or you can open Support Request to get help from VMware service professional.

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

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 Installation Logs for vCenter Server Appliance

You can collect installation log files and check these files to identify the source of a failure if vCenter Server Appliance stops responding during initial startup.

### Procedure

1 Access the appliance shell.

| Option | Description |
|---|---|
| **If you have direct access to the appliance** | Press Alt+F1. |
| **To connect remotely** | Use SSH or another remote console connection to start a session to the appliance. |

2 Enter a user name and password that the appliance recognizes.

3 In the appliance shell , run the `pi shell` command to access the Bash shell.

4 In the Bash shell, run the `vc-support.sh` script to generate a support bundle.

This command generates a `.tgz` file in `/var/tmp`.

5 Export the generated support bundle to the `user@x.x.x.x:/tmp` folder.

```
scp /var/tmp/vc-etco-vm-vlan11-dhcp-63-151.eng.vmware.com-2014-02-28--21.11.tgz
user@x.x.x.x:/tmp
```

6 Determine which `firstboot` script failed.

```
cat /var/log/firstboot/firstbootStatus.json
```

### What to do next

To identify potential causes of the failure, examine the log file of the `firstboot` script that failed.

## Collect Database Upgrade Logs

You can retrieve the database upgrade log files manually for examination.

You can retrieve the database upgrade logs after you complete the vCenter Server upgrade process.

### Prerequisites

### Procedure

1 Navigate to the database upgrade log locations.

2 Open the database upgrade logs in a text editor for examination.

### Results

You can examine the log files for the details of your database upgrade process.

## Example: Database Upgrade Locations

- For pre-upgrade checks, review the `%TEMP%\..\vcsUpgrade\vcdb_req.out` file.

The vcdb_req.err file tracks any errors that were identified during the pre-upgrade phase.

- For export details, review the `%TEMP%\..\vcsUpgrade\vcdb_export.out` file.

  The vcdb_export.err file contains errors that were identified during the export phase of the upgrade.

- For import details, review the `ProgramData\Vmware\CIS\logs\vmware\vpx\vcdb_import.out` file.

  The vcdb_import.err file contains errors that were identified during the import phase of the upgrade process.

- For in-place upgrade log details, review the `ProgramData\Vmware\CIS\logs\vmware\vpx\vcdb_inplace.out` file.

  The vcdb_inplace.err file contains in-place upgrade errors.

**What to do next**

Examine the vcdb_inplace.* log files.

# Collect Logs to Troubleshoot ESXi Hosts

You can collect installation or upgrade log files for ESXi. If an installation or upgrade fails, checking the log files can help you identify the source of the failure.

**Solution**

1. Enter the `vm-support` command in the ESXi Shell or through SSH.
2. Navigate to the `/var/tmp/` directory.
3. Retrieve the log files from the `.tgz` file.

# Errors and Warnings Returned by the Installation and Upgrade Precheck Script

The installation and upgrade precheck script runs tests to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log file.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

Table 12-1. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script

| Error or Warning | Description |
|---|---|
| 64BIT_LONGMODESTATUS | The host processor must be 64-bit. |
| COS_NETWORKING | Warning. An IPv4 address was found on an enabled service console virtual NIC that has no corresponding address in the same subnet in the vmkernel. A separate warning appears for each such occurrence. |
| CPU_CORES | The host must have at least two cores. |
| DISTRIBUTED_VIRTUAL_SWITCH | If the Cisco Virtual Ethernet Module (VEM) software is found on the host, the test checks that the upgrade also contains the VEM software. The test also determines whether the upgrade supports the same version of the Cisco Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the test returns a warning. The result indicates which version of the VEM software was expected on the upgrade ISO and which versions, if any, were found. You can use ESXi Image Builder CLI to create a custom installation ISO that includes the appropriate version of the VEM software. |
| HARDWARE_VIRTUALIZATION | Warning. If the host processor doesn't have hardware virtualization or if hardware virtualization is not turned on in the host BIOS, host performance suffers. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation. |
| MD5_ROOT_PASSWORD | This test checks that the root password is encoded in MD5 format. If a password is not encoded in MD5 format, it might be significant only to eight characters. In this case, any characters after the first eight are no longer authenticated after the upgrade, which can create a security issue. To work around this problem, see VMware knowledge base article 1024500. |
| MEMORY_SIZE | The host requires the specified amount of memory to upgrade. |
| PACKAGE_COMPLIANCE | vSphere Update Manager only. This test checks the existing software on the host against the software contained on the upgrade ISO to determine whether the host has been successfully upgraded. If any of the packages are missing or are an older version than the package on the upgrade ISO, the test returns an error and indicates which software was found on the host and which software was found on the upgrade ISO. |
| PARTITION_LAYOUT | You can upgrade or migrate software only if at most one VMFS partition on the disk is being upgraded and the VMFS partition must start after sector 1843200. |

Table 12-1. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (continued)

| Error or Warning | Description |
|---|---|
| POWERPATH | This test checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the test checks that matching components,such as CIM, vmkernel and module, also exist in the upgrade. If they do not exist, the test returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found. |
| PRECHECK_INITIALIZE | This test checks that the precheck script can be run. |
| SANE_ESX_CONF | The `/etc/vmware/esx.conf` file must exist on the host. |
| SPACE_AVAIL_ISO | vSphere Update Manager only. The host disk must have enough free space to store the contents of the installer CD or DVD. |
| SPACE_AVAIL_CONFIG | vSphere Update Manager only. The host disk must have enough free space to store the 5.x configuration between reboots. |
| SUPPORTED_ESX_VERSION | You can upgrade or migrate to ESXi 6.0 only from version 5.x ESXi hosts. |
| TBOOT_REQUIRED | This message applies only to vSphere Update Manager upgrades. The upgrade fails with this error when the host system is running in trusted boot mode (tboot), but the ESXi upgrade ISO does not contain any tboot VIBs. This test prevents an upgrade that can make the host less secure. |
| UNSUPPORTED_DEVICES | Warning. This test checks for unsupported devices. Some PCI devices are not supported in ESXi 6.0. |
| UPDATE_PENDING | This test checks the host for VIB installations that require a reboot. This test fails if one or more such VIBs is installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to reliably determine which packages are currently installed on the host, so it might not be safe to rely on the rest of the precheck tests to determine whether an upgrade is safe.<br>If you encounter this error, restart the host and retry the upgrade. |

# Restore vCenter Server Services If Upgrade Fails

If an upgrade to vCenter Server with external Platform Services Controller fails, you must manually restore or repoint vCenter Inventory Service or other vCenter Server services.

### Problem

If a vCenter Server upgrade failure occurs after the uninstallation phase and reverts the setup to the previous state (vCenter Server 5.1 or 5.5), it might not reregister vCenter Inventory Service or other vCenter Server services with the vCenter Single Sign-On included in Platform Services Controller 6.0.

### Cause

vCenter Inventory Service and other vCenter Server services are unregistered from vCenter Single-Sign-On 5.1 or 5.5 during the upgrade to vCenter Server 6.0. If an upgrade failure occurs after the services are unregistered, the registration information is lost. When the upgrade to vCenter Server 6.0 is resumed, the installer sees unregistered services and leaves them unregistered. The vCenter Inventory Service or other vCenter Server services must be manually repointed or registered with the newly upgraded Platform Services Controller 6.0 instance. See Knowledge Base article 2033620.

### Solution

- Find and follow the instructions in the knowledge base article for repointing or reregistering these services with vCenter Single Sign-On.

## VMware Component Manager Error During Startup After vCenter Server Appliance Upgrade

vCenter Server Appliance Component Manager fails with an error when you first deploy it after an upgrade.

### Problem

You deploy a vCenter Server Appliance instance and receive an error such as the following text:

"Firstboot script execution Error."

"The SSL certificate does not match when connecting to the vCenter Single Sign-On: hostname in certificate didn't match: <vcenter-b.domain.com> != <localhost.localdom> OR <localhost.localdom> OR <localhost>"

### Cause

The vCenter Server Appliance instance names do not match the names in the SSL certificates. You must regenerate the certificates to get the correct Fully Qualified Domain Names.

### Solution

1. Power on the vCenter Server Appliance 5.5 instance.
2. Log into the VAMI https://IP:5480.
3. Make sure that the correct IP address and Hostname are set in the Network Settings.
4. Select the Certificate regeneration check box.

5 Restart the vCenter Server Appliance 5.5 instance.

The vCenter Server, vSphere Web Client, vami, slapd, vCenter Inventory Service, and vCenter Single Sign-On certificates are regenerated with a certificate containing CN=vcenter-a.domain.com and SubjectAltName containing DNS=vcenter-a.domain.com DNS=vcenter-a IP=*192.168.2.100*.The certificates no longer contain *vcenter-b.domain.com*.

6 Rerun the vCenter Server Appliance 6.0 upgrade.

### Solution

See Upgrade the vCenter Server Appliance with Embedded vCenter Single Sign-On.

## 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?.