vSphere Upgrade

Update 2
Modified on 05 May 2022
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5

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.

vSphere Web Client and vSphere Client

Task instructions in this guide are based on the vSphere Web Client. You can also perform most of the tasks in this guide by using the new vSphere Client. The new vSphere Client user interface terminology, topology, and workflow are closely aligned with the same aspects and elements of the vSphere Web Client user interface. You can apply the vSphere Web Client instructions to the new vSphere Client unless otherwise instructed.

Note Not all functionality in the vSphere Web Client has been implemented for the vSphere Client in the vSphere 6.5 release. For an up-to-date list of unsupported functionality, see *Functionality Updates for the vSphere Client Guide* at http://www.vmware.com/info?id=1413.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Updated Information

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

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

Revision	Description
02 APR 2021	■ Updated the list of supported browser versions for the vSphere Web Client in vSphere Web Client Software Requirements. ■ 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.
29 APR 2020	Added the prerequisite that, when upgrading or migrating vCenter Server, you must create a backup of the existing vCenter Server or Platform Services Controller nodes in your environment. You can use the backup as a precaution in case there is a failure during the deployment process. See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance and Prerequisites for Migrating vCenter Server and Platform Services Controller.
04 MAY 2018	■ Updated the description of ports 80 and 443 in Required Ports for vCenter Server and Platform Services Controller. ■ Removed the HTTP and HTTPS custom port option from Stage 1 - Deploy the OVA File of the New vCenter Server Appliance With an Embedded Platform Services Controller, Stage 1 - Deploy the OVA File of the New Platform Services Controller Appliance, and Stage 1 - Deploy the OVA File of the New vCenter Server Appliance With an External Platform Services Controller. The custom port option is only available during the installation of vCenter Server 6.5 Update 2. You cannot customize the HTTP and HTTPS port numbers when upgrading to vCenter Server 6.5 Update 2. ■ Removed the custom port option from Deploy the OVA File for Migrating to the Target vCenter Server Appliance with an Embedded Platform Services Controller, Deploy the OVA File for Migrating to a Platform Services Controller Appliance, and Deploy the OVA File for the Target vCenter Server Appliance with an External Platform Services Controller. The custom port option is only available during the installation of vCenter Server 6.5 Update 2. You cannot customize the HTTP and HTTPS port numbers when migrating from a Windows-based vCenter Server to vCenter Server Appliance 6.5 Update 2. However, with vCenter Server 6.5 Update 2, you can migrate vCenter Server installed on Windows with custom HTTP and HTTPS ports to vCenter Server Appliance, and the custom port values are retained. By default, the vCenter Server HTTP and HTTPS ports are 80 and 443.
03 MAY 2018	Initial release.

Introduction to vSphere Upgrade 1

vSphere 6.5 provides many options for upgrading your vSphere deployment. For a successful vSphere upgrade, you must understand the upgrade options, the configuration details that impact the upgrade process, and the sequence of tasks.

The two core components of vSphere are VMware ESXi™ and VMware vCenter Server™. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. You use the vCenter Server system to pool and manage the resources of multiple hosts. vCenter Server Appliance is a preconfigured Linux OS--based virtual machine optimized for running the vCenter Server system and the vCenter Server components.

Starting with vSphere 6.0, important required services for running vCenter Server and the vCenter Server components are included in the Platform Services Controller.

Based on your existing vCenter Server configuration details, you can upgrade to one of the following deployment types:

- vCenter Server with an embedded Platform Services Controller.
- vCenter Server with an external Platform Services Controller.

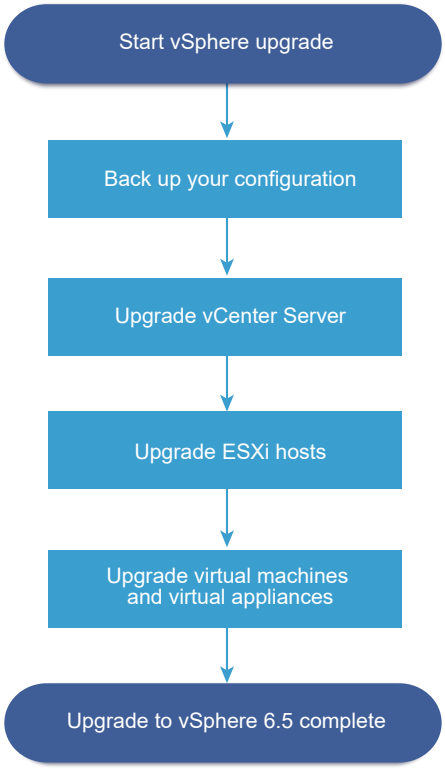
Important You cannot change your vCenter Server deployment type during upgrade.

This chapter includes the following topics:

Overview of the vSphere Upgrade Process

vSphere is a sophisticated product with multiple components to upgrade. Understanding the required sequence of tasks is vital for a successful vSphere upgrade.

Figure 1-1. Overview of High-Level vSphere Upgrade Tasks



Upgrading vSphere includes the following tasks:

1 Read the vSphere release notes.

2 Verify that you have backed up your configuration.

3 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

4 Upgrade vCenter Server. See Overview of the vCenter Server Upgrade Process.

5 If you are using vSphere Update Manager, upgrade it. Refer to the VMware vSphere Update Manager documentation.

6 Upgrade your ESXi hosts. See Overview of the ESXi Host Upgrade Process.

7 To ensure sufficient disk storage for log files, consider setting up a syslog server for remote logging. 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.

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

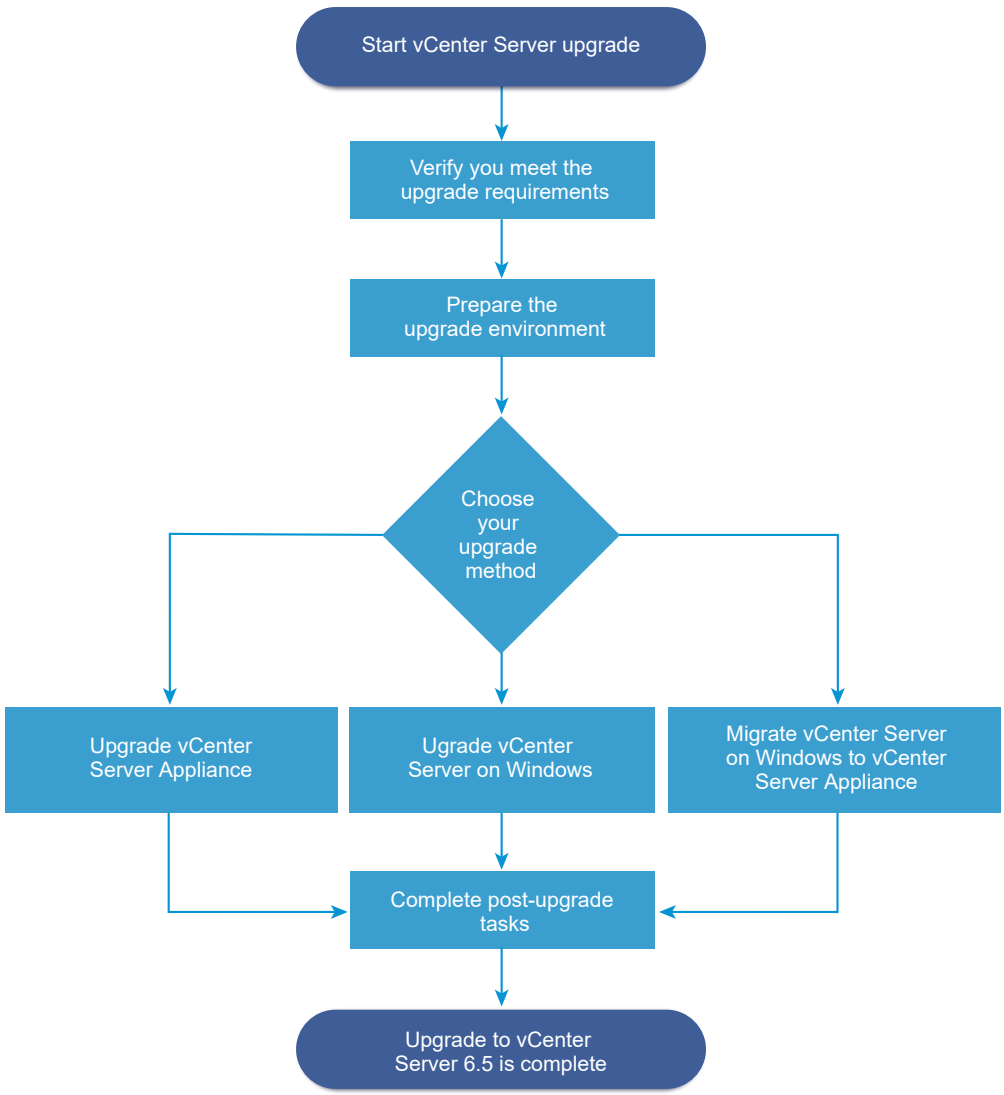
When you upgrade vSphere, you must perform all procedures in sequence to avoid possible data loss and to minimize downtime. You can perform the upgrade process for each component in only one direction. For example, after you upgrade to vCenter Server 6.5, you cannot revert to vCenter Server version 5.5 or version 6.0. With backups and some planning, however, you can restore your original software records.

Overview of the vCenter Server Upgrade Process

VMware provides many options to upgrade to vCenter Server 6.5.

You can upgrade or migrate your vCenter Server version 5.5 or version 6.0 installation to version 6.5 using the method that best addresses your deployment goals and requirements.

Figure 1-2. vCenter Server High-level Upgrade Tasks



High-level steps for upgrading or migrating vCenter Server:

1 Select your upgrade goal.

- Chapter 2 Upgrading the vCenter Server Appliance and Platform Services Controller Appliance
- Chapter 3 Upgrading vCenter Server for Windows
- Chapter 4 Migrating vCenter Server for Windows to vCenter Server Appliance

2 Verify that your system meets the hardware and software requirements.

3 Prepare your environment for the upgrade or migration.

4 Upgrade or migrate your vCenter Server for Windows or vCenter Server Appliance deployment.

5 Complete any required post-upgrade or post-migration tasks.

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

Important Although you can choose 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 5.5 instance, see Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration. For information on upgrade order for transitional environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

vCenter Server Supported Upgrade Methods

Graphical User Interface (GUI) Installer

The GUI installer provides a two-step upgrade method using OVA and the vCenter Server Appliance Management GUI. The first step deploys an unconfigured Platform Services Controller appliance or vCenter Server Appliance as an OVA file. The second step uses the vCenter Server Appliance Management GUI to configure the new appliance using the source deployment data.

Command Line Interface (CLI) Installer

The CLI installer provides advanced users with a CLI method for upgrading the vCenter Server Appliance or migrating vCenter Server on Windows to an appliance. You can upgrade or migrate to vCenter Server Appliance configurations using customized CLI templates.

Migration Assistant Interface for Migrating vCenter Server on Windows to vCenter Server Appliance

When you migrate a legacy vCenter Single Sign-On, Platform Services Controller, or vCenter Server on Windows to an appliance using the Migration Assistant interface. You can use either the GUI method or the CLI method to migrate the legacy Windows installation data to a target appliance. See Overview of Migration from vCenter Server on Windows to an Appliance.

Deprecated vCenter Server Deployment Models

When upgrading or migrating from deprecated deployment models, you must first migrate your deployment to a currently supported deployment model before attempting to upgrade or migrate it to a vCenter Server 6.5 deployment. For more information, see Moving from a Deprecated to a Supported vCenter Server Deployment Topology Before Upgrade or Migration

Patching and Updating vCenter Server

A patch or update brings the vCenter Server 6.5 software up to the current minor version on the existing physical or virtual machine. You can use the patching process to make minor upgrades to your 6.5 deployment. See Differences Between vSphere Upgrades, Patches, Updates, and Migrations and Chapter 7 Patching and Updating vCenter Server 6.5 Deployments.

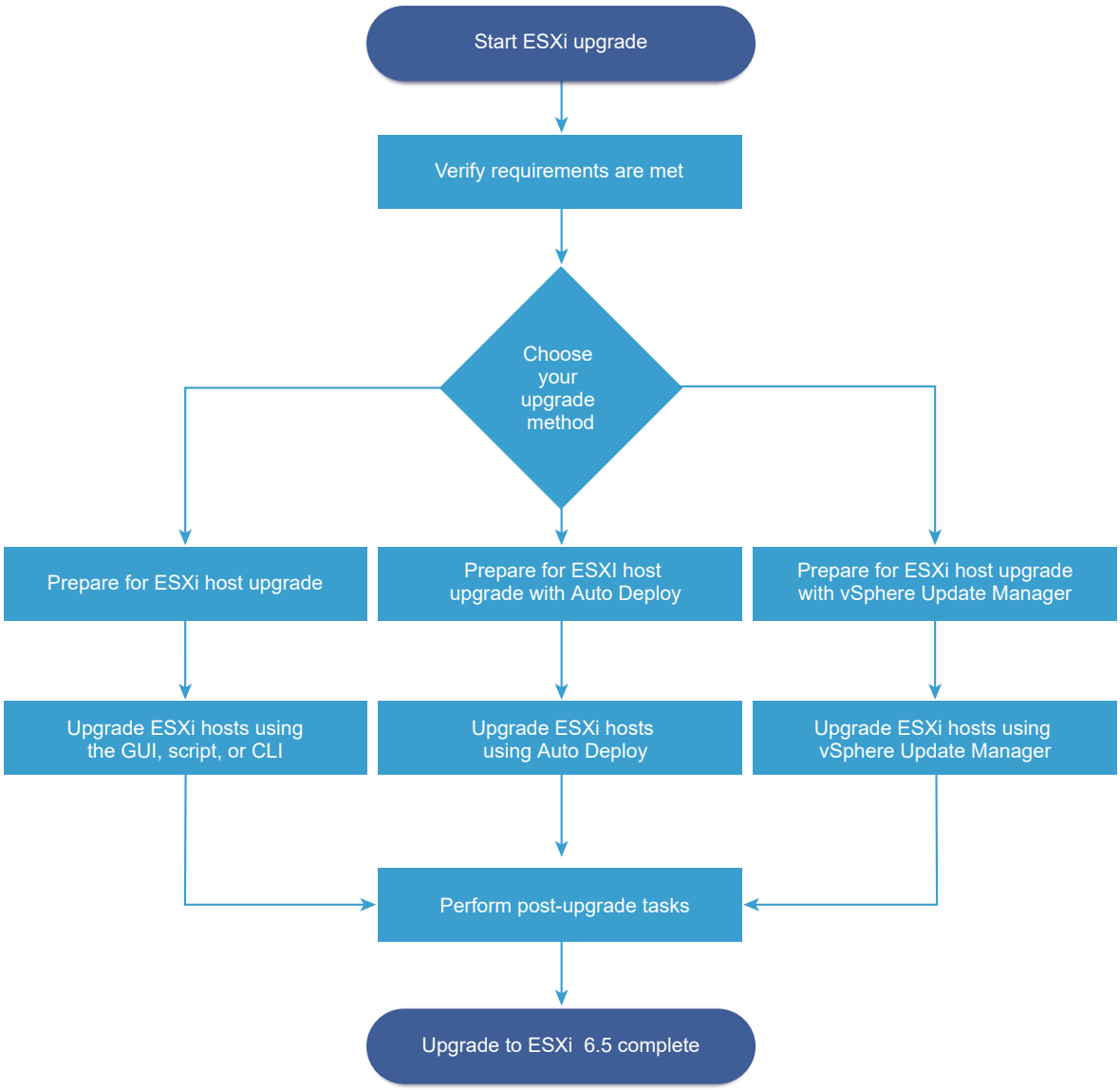
Overview of the ESXi Host Upgrade Process

VMware provides several ways to upgrade ESXi version 5.5.x and version 6.0.x hosts to ESXi 6.5.

The details and level of support for an upgrade to ESXi 6.5 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 5.5.x host or 6.0.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 5.5.x host or 6.0.x host that has custom VIBs to version 6.5, the custom VIBs are migrated. See Upgrading Hosts That Have Third-Party Custom VIBs.

Figure 1-3. Overview of the ESXi Host Upgrade Process



High level steps for upgrading ESXi:

1 Verify that your system meets the upgrade requirements. See ESXi Requirements.

2 Prepare your environment before upgrading. See Before Upgrading ESXi Hosts.

3 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.

4 Upgrade ESXi. See Chapter 8 Upgrading ESXi Hosts

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

Methods supported for direct upgrade to ESXi 6.5 are:

- Use the interactive graphical user interface (GUI) installer from CD, DVD, or USB drive.
- Scripted upgrade.
- Use the `esxcli` command line interface (CLI).
- vSphere Auto Deploy. If the ESXi 5.5.x host was deployed by using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a 6.5 image.
- vSphere Update Manager.

Graphical User Interface (GUI) Installer

Upgrade interactively by using an ESXi installer ISO image on CD/DVD or USB flash drive. You can run the ESXi 6.5 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 6.5. 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 5.5.x and ESXi 6.0.x to ESXi 6.5 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.

esxcli Command Line Interface

You can use the `esxcli` command-line utility for ESXi to upgrade ESXi 5.5.x hosts or ESXi 6.0.x hosts to ESXi 6.5 hosts. See Upgrading Hosts by Using esxcli Commands .

vSphere Auto Deploy

After an ESXi 5.5.x or ESXi 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 Chapter 9 Using vSphere Auto Deploy to Reprovision Hosts .

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 virtual machine upgrade, see the *Installing and Administering VMware vSphere Update Manager* documentation.

The `esxupdate` and `vihostupdate` utilities are not supported for ESXi 6.5 upgrades.

Upgrading Virtual Machines and VMware Tools

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.

vCenter Server Upgrade Compatibility

The upgrade to vCenter Server 6.5 affects other software components of the data center.

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

vCenter Server 6.5 can manage ESXi version 5.5 or 6.0 hosts in the same cluster with ESXi 6.5 hostsvCenter Server 6.5 cannot manage ESXi 5.1 or earlier hosts.

You cannot upgrade to vCenter Server 6.5 from vCenter Server 5.1 or earlier. You must first upgrade to vCenter Server version 5.5 or 6.0.

Table 1-1. 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. **Note** vCenter Server Appliance for vCenter Server 6.5 uses PostgreSQL for the embedded database. vCenter Server Appliance 6.5 does not support external databases.

Table 1-1. Upgrading vCenter Server and Related VMware Products and Components (continued)

Product or Component	Compatibility
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.
VMFS-3 volumes	You can continue to use existing VMFS-3 datastores, but you cannot create VMFS-3 datastores. If you have VMFS-3 datastores, upgrade them to VMFS-6.
Virtual machines	Upgrade options depend on your current version. See Upgrading Virtual Machines and VMware Tools.
VMware Tools	Upgrade options depend on your current version. See the information about upgrading VMware Tools in Upgrading Virtual Machines and VMware Tools.
Auto Deploy	To ensure compatibility and best performance, when you upgrade to vCenter Server 6.5, use Auto Deploy to upgrade ESXi hosts to the same version.

vSphere 6.5 Component Behavior Changes that Affect Upgrade

When upgrading to vSphere 6.5, it is important to understand changes in component behavior for version 6.5 that can affect the upgrade process.

Understanding changes from previous versions of vSphere can assist in your upgrade planning. For a complete list of new features in vSphere 6.5, see the Release Notes for version 6.5 releases.

vCenter Server Upgrade Methods

vSphere supports multiple methods for upgrading vCenter Server to version 6.5.

Supported Migration Path from vCenter Server for Windows to vCenter Server Appliance

You can migrate from an existing vCenter Server for Windows configuration to a vCenter Server Appliance 6.5 deployment using a graphical user interface-based installer or a command line interface-based installer. See Differences between Upgrading and Migrating vCenter Server on Windows.

Support for Command Line Interface (CLI) Deployments of vCenter Server Appliance

You can upgrade an existing vCenter Server Appliance deployment to version 6.5 using a CLI. See CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance.

VMware Update Manager Changes

You can use a graphical user interface (GUI) when upgrading vCenter Server deployments using VMware Update Manager.

Simple Upgrade Process from vCenter Server 5.5 Replaced

Upgrading from vCenter Server 5.5 to vCenter Server 6.5 with an embedded Platform Services Controller instance replaces the vCenter Server5.5 simple upgrade process. The upgrade process migrates your vCenter Server 5.5 services to a vCenter Server 6.5 deployment with an embedded Platform Services Controller instance.

Custom Upgrade Process from vCenter Server 5.5 Replaced

Upgrading from vCenter Server 5.5 to vCenter Server 6.5 with an external Platform Services Controller instance replaces the vCenter Server 5.5 Custom or separate upgrade process. When you upgrade your custom or distributed vCenter Server 5.5 instance, the upgrade process includes any vCenter Server 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 6.5 with an external Platform Services Controller deployment, any vCenter Server 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 Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration

Upgrade Order and Mixed Version Environment Behavior

You cannot upgrade multiple vCenter Server instances or Platform Services Controller instances concurrently, and upgrade order matters. See Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Changes in Supported Deployment Types

Changes from previous versions of vSphere can affect your deployment type.

VMware Platform Services Controller Changed from vCenter Server 5.5

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.

vCenter Server Component Services Deployment Changed from vCenter Server 5.5

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.

vCenter Server 5.5 services that are deployed individually before the upgrade are migrated to the appropriate service group during the upgrade process. The upgrade software migrates, upgrades, and configures existing vCenter Server 5.5 services as needed.

- vCenter Single Sign-On credentials, certificates, and ports are migrated to the Platform Services Controller instance.
- Tagging data and licensing is migrated to the Platform Services Controller instance.
- Other services are migrated to the vCenter Server instance. For details, see Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration.
- You can now choose the destination folder for the upgrade software to use.

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

Enhanced Linked Mode Topology Changes from vCenter Server 5.5

The implementation of Linked Mode has changed starting with vSphere 6.0. 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.

Topology Changes After Upgrade or Migration

You can change your deployment topology after upgrade or migration to vCenter Server 6.5. You cannot change your deployment type during upgrade or migration. For information on supported topology changes, see Chapter 6 Changing a vCenter Server Deployment Type After Upgrade or Migration.

Mixed IPv4 and IPv6 Upgrade and Migration

- Upgrade and migration from vCenter Server 6.0 to 6.5 is supported for pure IPv4 or pure IPv6 management networks only.
- Upgrade and migration from vCenter Server 5.5 to 6.5 supports only IPv4. You can reconfigure the target deployment to IPv6 after upgrading or migrating.

- Upgrade and migration from a mixed mode IPv4 and IPv6 environment transfers configurations depending on the source deployment configuration.

  Table 1-2. Transfer of networking configuration settings for mixed mode IPv4 and IPv6 deployments

Source configuration	Settings transferred during upgrade or migration	Settings not transferred during upgrade or migration
DHCPv6 and AUTOv6	DHCPv6	AUTOv6
DHCPv4 and DHCPv6	DHCPv4	DHCPv6
DHCPv4 and AUTOv6	DHCPv4	AUTOv6
DHCPv4 and Static IPv6	Static IPv6	DHCPv4
Static IPv4 and AUTOv6	Static IPv4	AUTOv6
Static IPv4 and DHCPv6	Static IPv4	DHCPv6
Static IPv4 and Static IPv6	Static IPv4 and Static IPv6	-

Changes Affecting VMware Services

Changes affecting VMware services may affect your upgrade planning.

Embedded PostgreSQL Database Replaces Embedded Microsoft SQL Server Express Database for vCenter Server 6.0

The vCenter Server 6.0 embedded Microsoft SQL Server Express database is replaced with an embedded PostgreSQL database during the upgrade to vCenter Server 6.5. The maximum inventory size that applied for Microsoft SQL Server Express still applies for PostgreSQL.

vCenter Inventory Services Removed for vCenter Server 6.5

vCenter Inventory Services are no longer needed for vCenter Server 6.5. The upgrade process migrates the data and removes the vCenter Inventory Services.

Using Oracle for vCenter Server External Database

For information about supported database server versions, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

VMware vSphere Syslog Collector

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

VMware Syslog Service

Starting with vCenter Server Appliance 6.0, vSphere Syslog Service is a support tool for logging that is included in the vCenter Server group of services.

Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments

When you upgrade or migrate a deployment with multiple vCenter Server instances, the upgrade or migration order matters.

You upgrade or migrate externally deployed vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances first. You temporarily leave the vCenter Server instances at version 5.5 or version 6.0 while you complete the upgrade or migration process for the vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances.

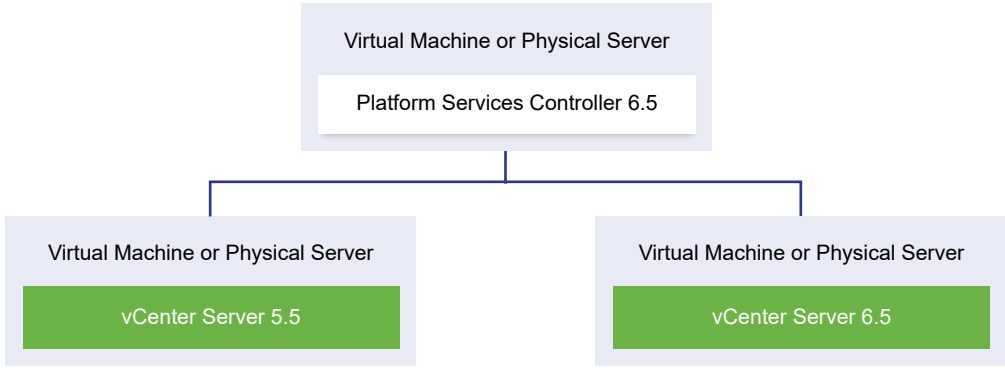
- You must upgrade or migrate your vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances sequentially.
- For a mixed-platform installation with vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances on Windows and vCenter Server Appliance instances, upgrade or migrate all the vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances on Windows before upgrading any vCenter Server Appliance instances.
- For a mixed-platform installation with vCenter Single Sign-On 5.5 appliances or Platform Services Controller 6.0 appliances and vCenter Server instances on Windows, upgrade all the vCenter Single Sign-On 5.5 appliances or Platform Services Controller 6.0 appliances before upgrading or migrating any vCenter Server instances on Windows.
- After upgrading or migrating your vCenter Single Sign-On 5.5 instances or Platform Services Controller 6.0 instances, you can upgrade vCenter Server instances. vCenter Server instances that point to the same Platform Services Controller can be upgraded or migrated concurrently.

When you upgrade an externally deployed vCenter Single Sign-On 5.5 instance or Platform Services Controller 6.0 instance to an externally deployed Platform Services Controller 6.5 instance, the legacy vCenter Server instances that were using the component are not affected. The legacy vCenter Server instances continue to operate with the upgraded Platform Services Controller just as they operated before the upgrade without any problems or required reconfiguration. Legacy vCenter Server instances continue to be visible to the legacy vSphere Web Client, though vCenter Server 6.5 instances are not visible to the legacy vSphere Web Clients.

Transitional behavior during a migration from a vCenter Server deployment on Windows to an appliance deployment is the same as for a vCenter Server upgrade on Windows.

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 1-4. Mixed-Version 5.5 and 6.5 Transitional Environment



Important Mixed-version environments are not supported for production. Use these environments only during the period when an environment is in transition between vCenter Server versions.

If you upgrade an external vCenter Single Sign-On 5.5 and at least one instance of vCenter Server to version 6.5 while leaving other instances of vCenter Server at version 5.5, expect the following behavior:

- 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 mixed-version 5.5 and 6.5 environment, a vSphere Web Client 6.5 instance shows vCenter Server 5.5 instances.
- vSphere Web Client 5.5 shows vCenter Server instances only, not 6.5 instances.

When you upgrade the external vCenter Single Sign-On 5.5 instance to an external Platform Services Controller 6.5 instance, and all vCenter Server 5.5 instances to version 6.5, 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 transitional order and behavior are the same for vCenter Server 6.0 environments when upgrading or migrating to vCenter Server 6.5 environments. The vCenter Server 6.0 instances continue operating with the Platform Services Controller 6.5 instance as they did before the upgrade or migration, without any problems or required action.

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

Figure 1-5. Example vSphere 5.5 Deployment Before Transition Begins

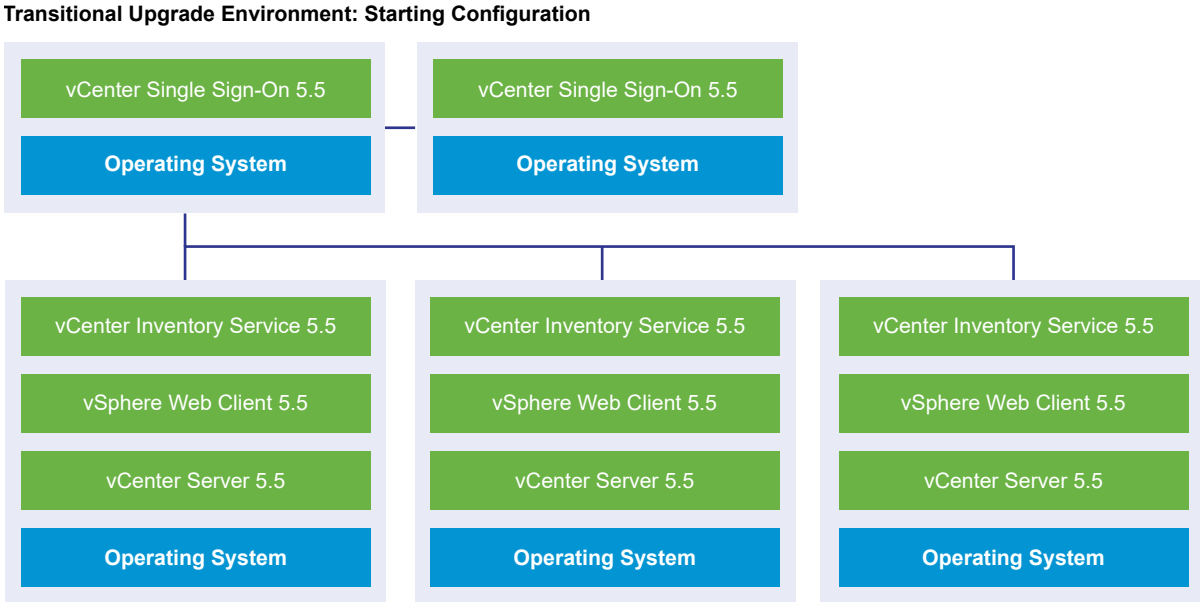
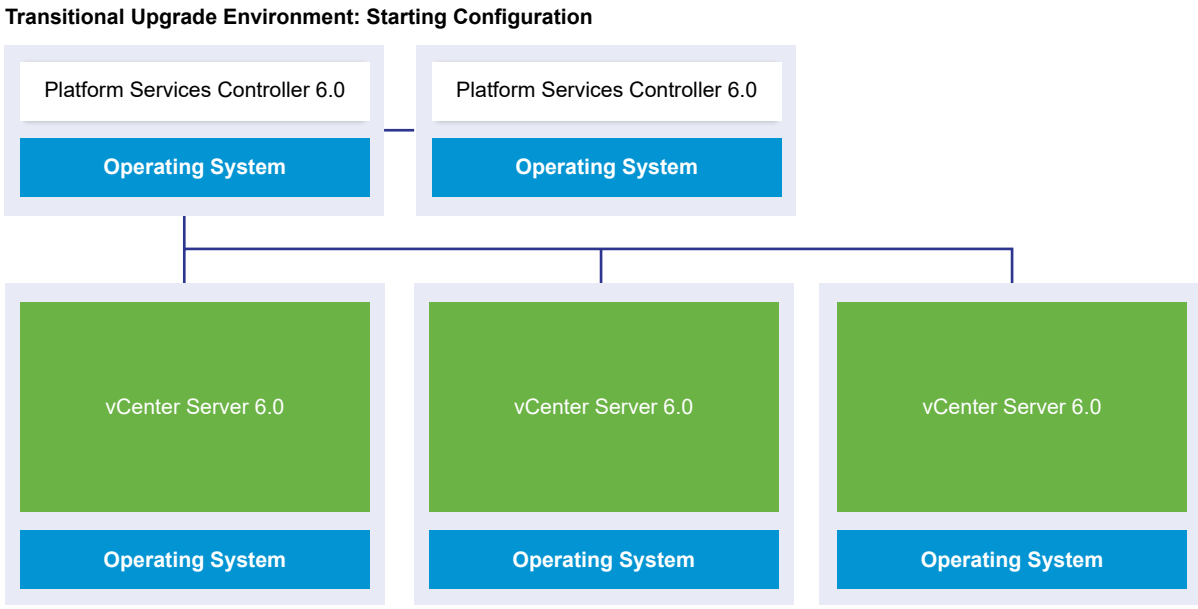


Figure 1-6. Example vSphere 6.0 Deployment Before Transition Begins



For example, a deployment with three vCenter Server instances and two external vCenter Single Sign-On instances must be upgraded or migrated one instance at a time to version 6.5.

Figure 1-7. Example vSphere 5.5 Deployment in Transition at Step 1

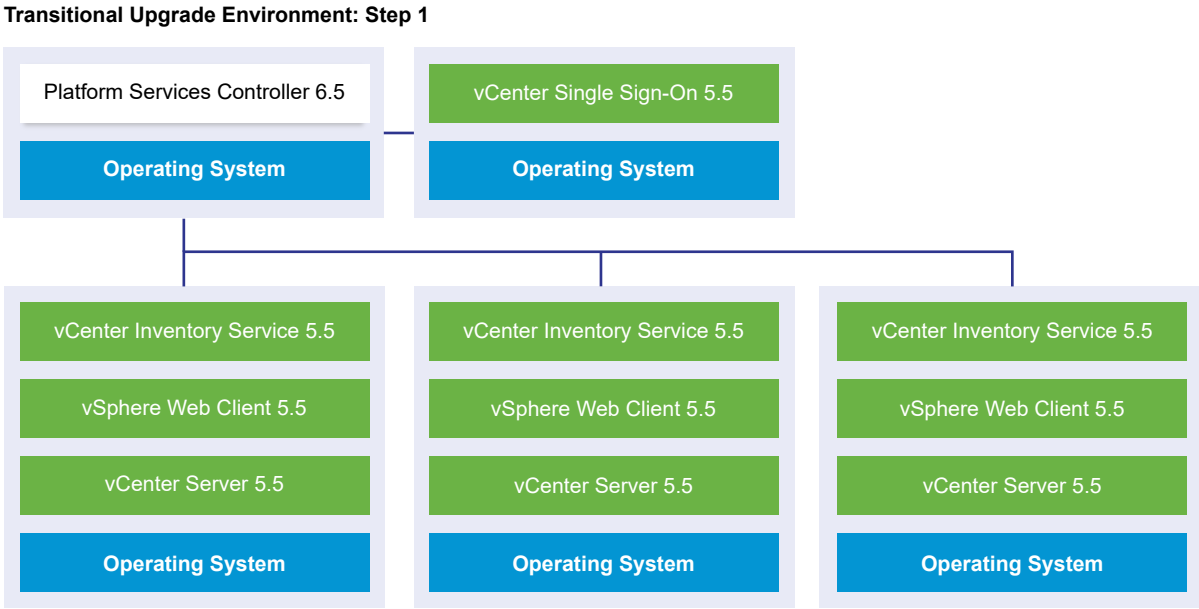
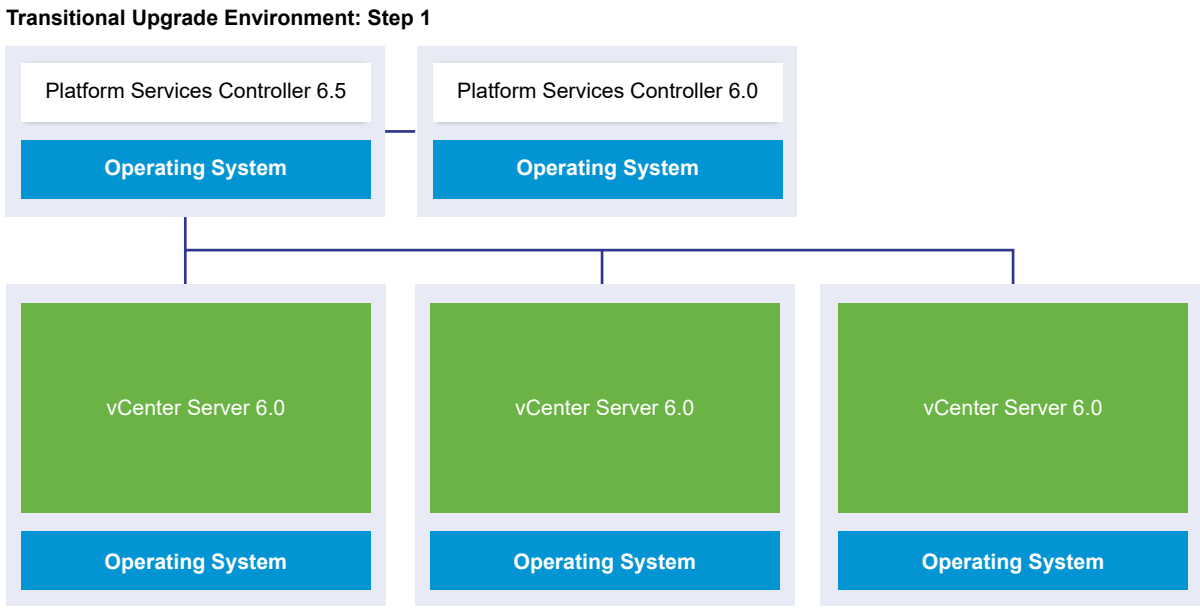


Figure 1-8. Example vSphere 6.0 Deployment in Transition at Step 1



Upgrading or migrating the first external vCenter Single Sign-On instance or Platform Services Controller instance to an external Platform Services Controller of the current version has no impact on the legacy vCenter Server instances except that Linked Mode no longer functions for version 5.5 instances.

Figure 1-9. Example vSphere 5.5 Deployment in Transition at Step 2

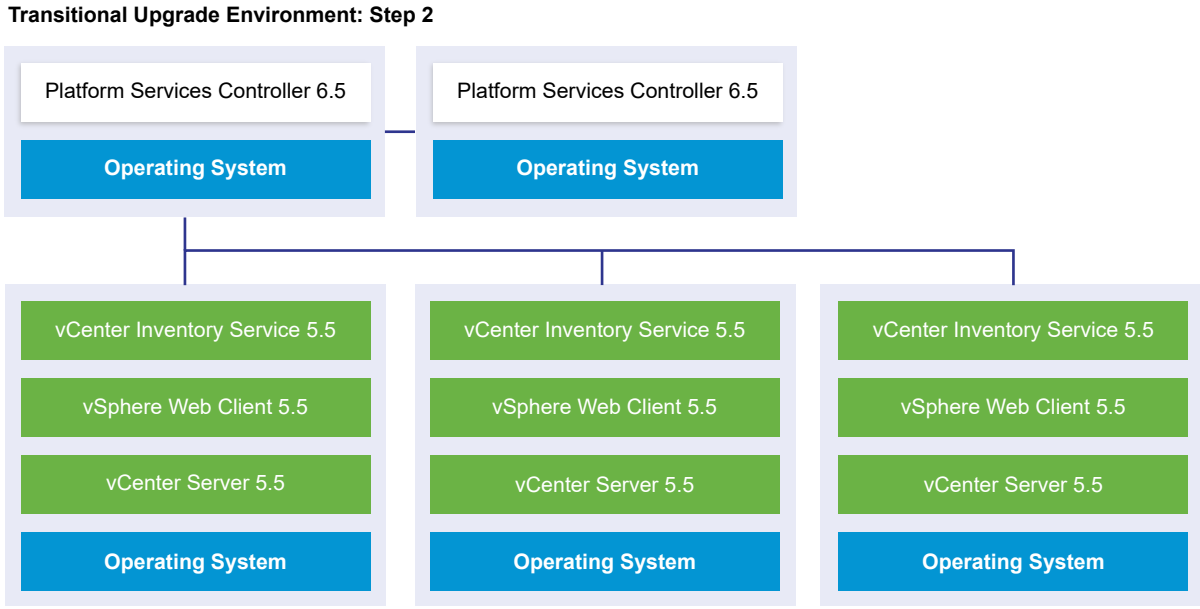
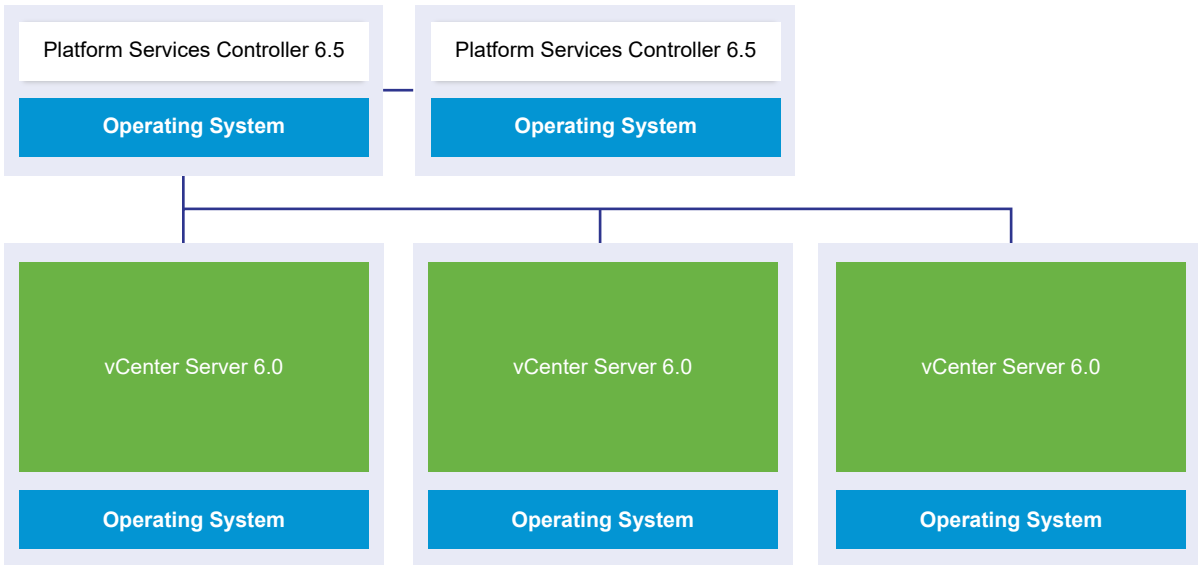


Figure 1-10. Example vSphere 6.0 Deployment in Transition at Step 2



Upgrading or migrating the second external vCenter Single Sign-On instance or Platform Services Controller instance to the current version has no impact on the behavior of the legacy vCenter Server instances.

Figure 1-11. Example vSphere 5.5 Deployment in Transition at Step 3

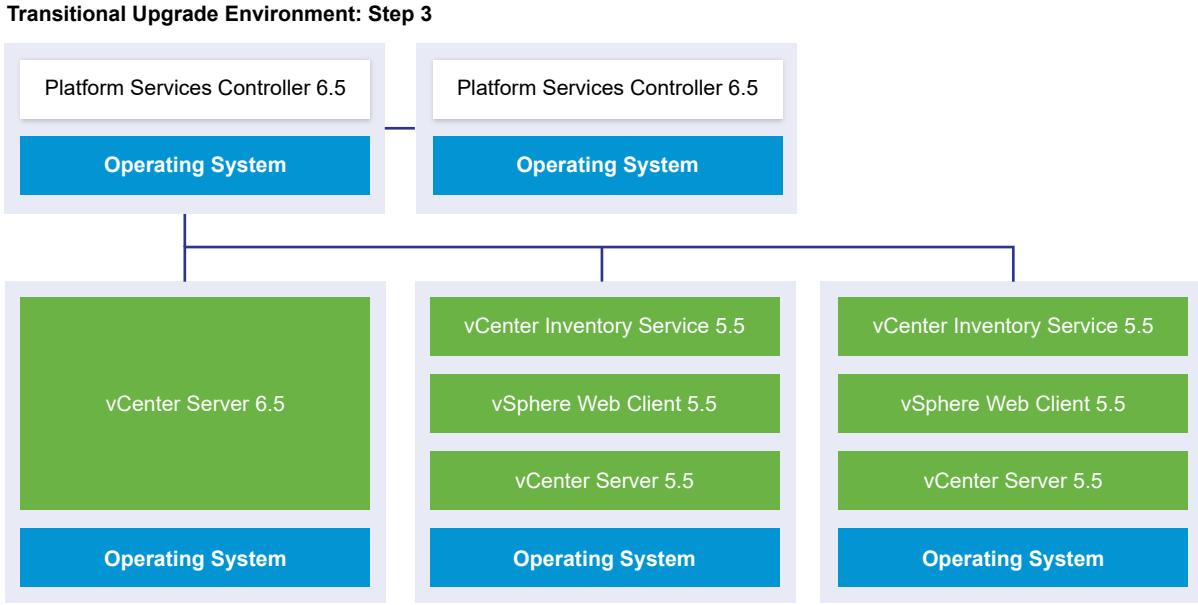
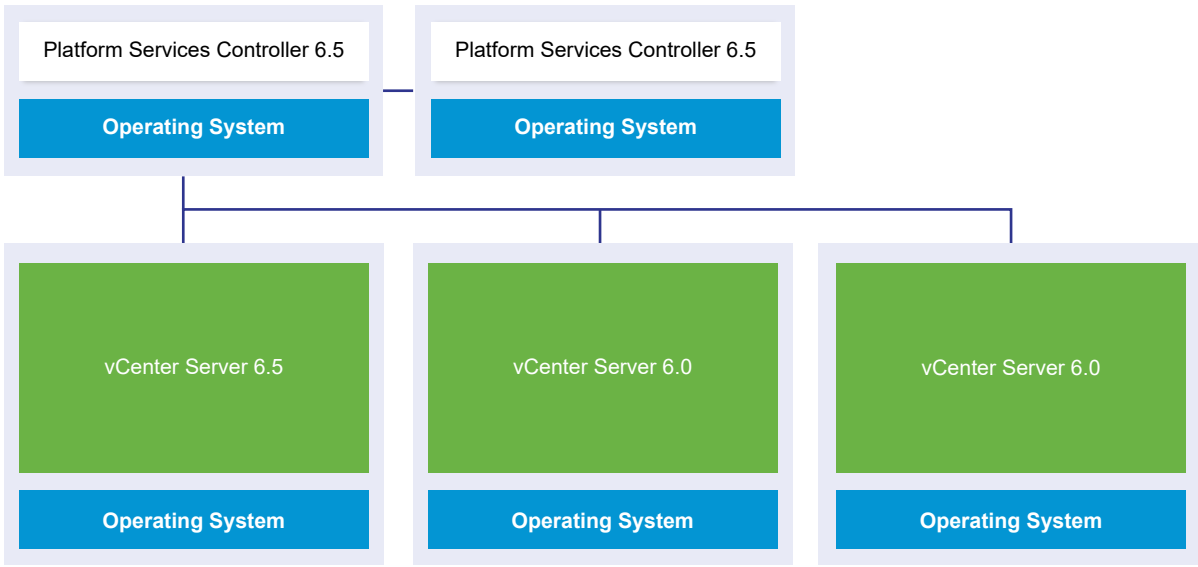


Figure 1-12. Example vSphere 6.0 Deployment in Transition at Step 3



After upgrading the first vCenter Server instance to 6.5, changes occur in the connectivity between the vCenter Server instances.

- The two remaining legacy vSphere Web Client instances can no longer view the newly upgraded vCenter Server 6.5 instance after it joins the Platform Services Controller instance.
- The legacy vSphere Web Client instances can still view the legacy vCenter Server instances after they are restarted.
- The vSphere Web Client 6.5 instance that is part of the newly upgraded vCenter Server 6.5 instance can view the legacy vCenter Server instances and 6.5 instances.

Figure 1-13. Example vSphere 5.5 Deployment in Transition at Step 4

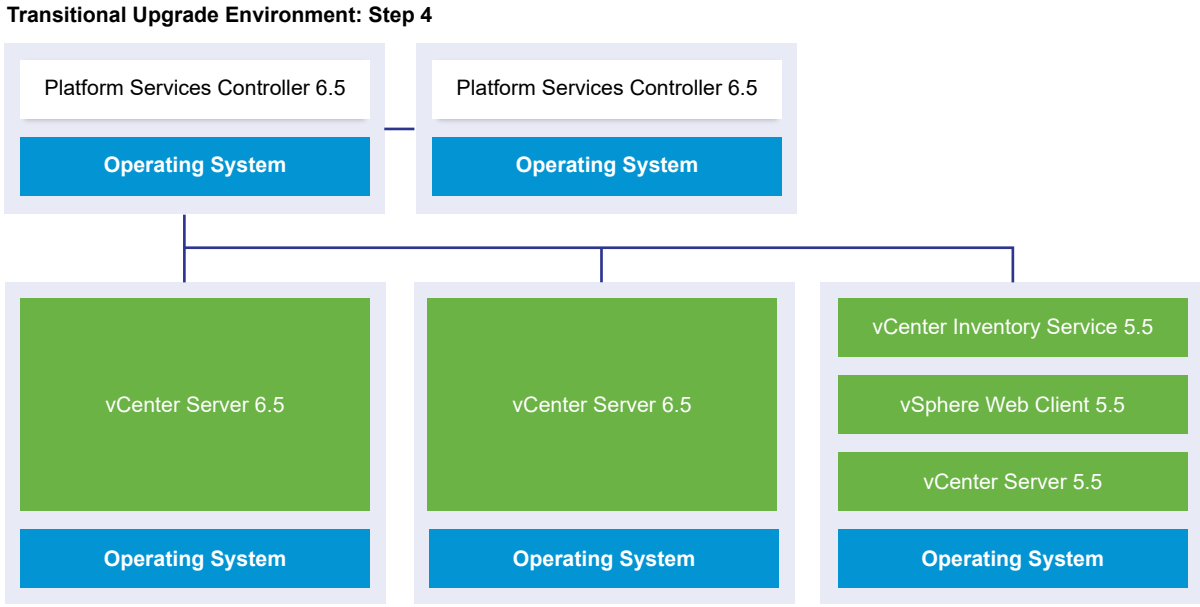
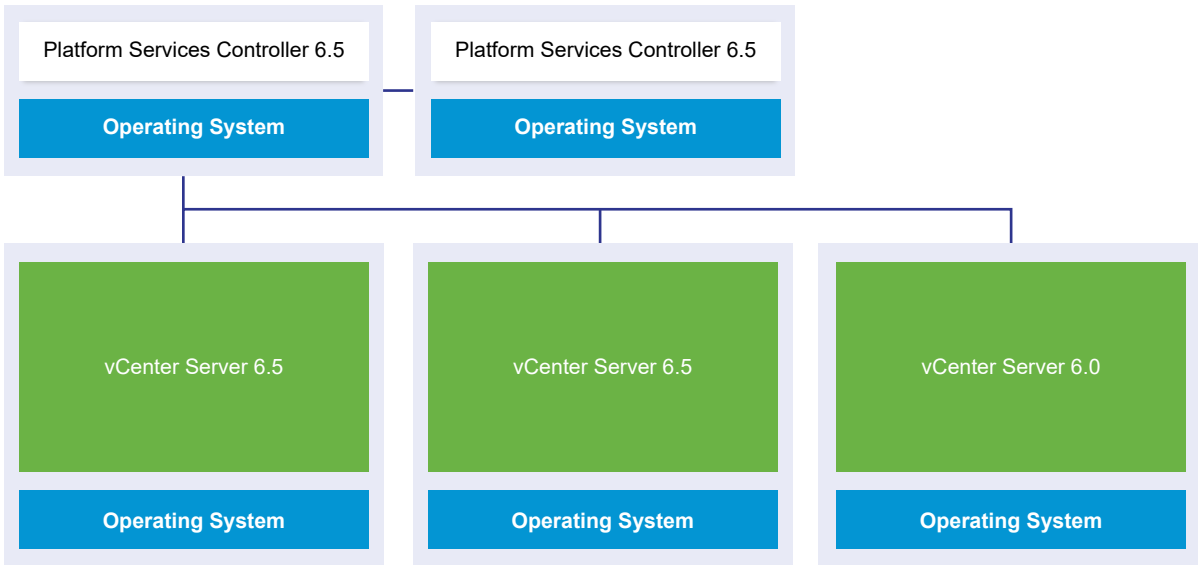


Figure 1-14. Example vSphere 5.5 Deployment in Transition at Step 4



After upgrading the second vCenter Server instance to 6.5, 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 6.5 instances after they are joined to the Platform Services Controller.
- The remaining legacy vSphere Web Client instance can no longer view the vCenter Server 6.5 instances.

- The legacy vSphere Web Client instance can still view the legacy vCenter Server instances after they are restarted.
- The vSphere Web Client 6.5 instances that are part of the newly upgraded vCenter Server 6.5 instances can view the legacy vCenter Server instances and 6.5 instances.

Figure 1-15. Example vSphere 5.5 Deployment After Step 5 with Upgrade Complete

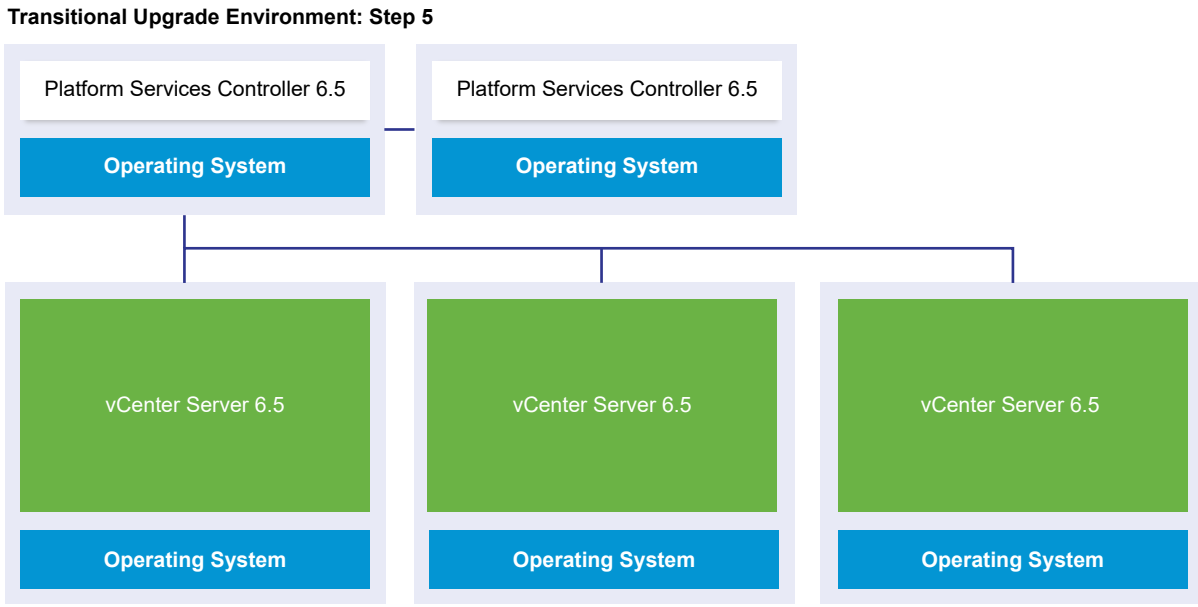
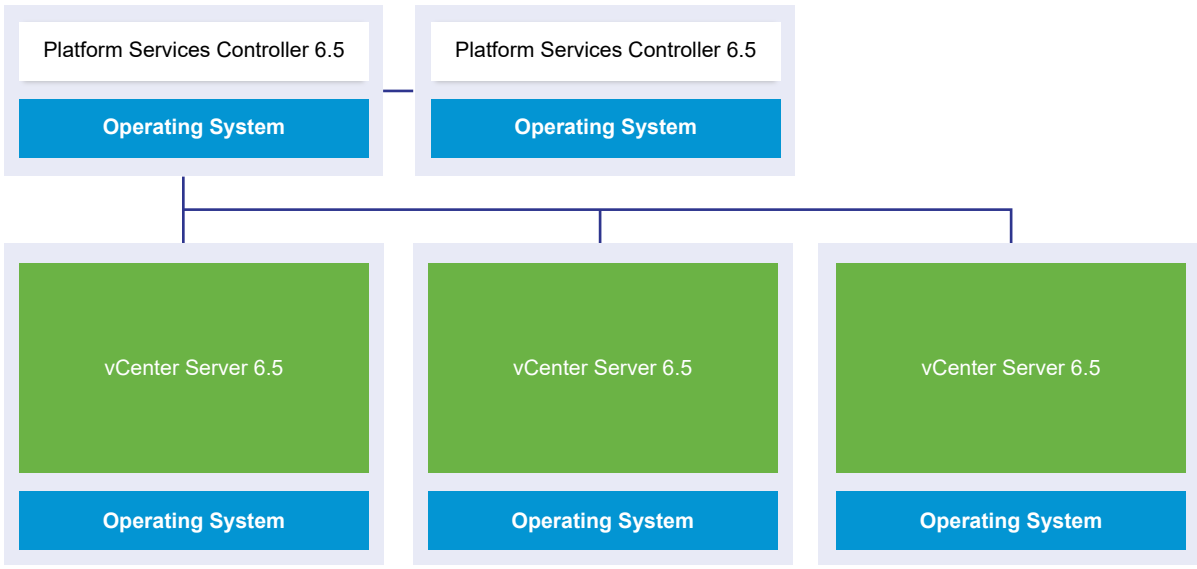


Figure 1-16. Example vSphere 6.0 Deployment After Step 5 with Upgrade Complete



After upgrading the third and final vCenter Server instance to 6.5, all the vCenter Server instances are connected with full vCenter Server 6.5 functionality.

- Enhanced Linked Mode functionality replaces Linked Mode functionality between all the legacy vCenter Server instances after they are joined to the Platform Services Controller 6.5 instances.
- The vSphere Web Client 6.5 instances can view all the vCenter Server 6.5 instances.

Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration

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

If all vCenter Server 5.5 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 upgrade and migration software relocates your service or services to the vCenter Server virtual machine or physical server during upgrade or migration. Some services require reconfiguration or other actions after upgrade or migration. These vCenter Server 5.5 for Windows services are relocated to become part of the vCenter Server group of services during the upgrade or migration process:

- vSphere Web Client
- vSphere Auto Deploy
- vSphere Syslog Collector
- vSphere ESXi Dump Collector
- vSphere Update Manager

vCenter Inventory Services functionality is replaced by the vCenter Content Library and other services which are part of vCenter Server 6.5. The upgrade or migration process migrates the data from vCenter Inventory Service to the new database support services in vCenter Server 6.5.

vSphere Syslog Collector functionality is replaced by vCenter Server services functionality.

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

Table 1-3. vCenter Server 5.5 Distributed Service Relocation 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	Replaced with vCenter Content Library as part of the vCenter Server services	vCenter Inventory Service 5.5 data is copied to the vCenter Content Library instance that is installed with vCenter Server 6.5. You do not need to copy it manually. vCenter Inventory Service 5.5 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 as part of the vCenter Server services	vCenter Server 5.5 data is copied to the vSphere Web Client 6.5 instance that is installed with vCenter Server 6.5. vSphere Web Client 5.5 is still running but is no longer used. It must be manually stopped and removed.
vSphere Auto Deploy	Not installed on the vCenter Server system	Relocated as part of the vCenter Server system	vSphere Auto Deploy data is copied to the Auto Deploy 6.5 instance that is installed with vCenter Server 6.5. Repoint vCenter Server DHCP settings to the migrated vSphere Auto Deploy service. vCenter Server vSphere Auto Deploy 5.5 is still running but is no longer used. It must be manually stopped and removed.
vSphere Syslog Collector	Not installed on the vCenter Server system	Relocated as part of the vCenter Server services Data is not retained. Configurations for ports, protocols, and rotation log size are preserved.	■ ESXi system information might remain on an old system until you relocate it. ■ 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 as part of the vCenter Server services Data is not retained.	■ ESXi core dump data might remain on an older system until you migrate it. ■ ESXi hosts might require reconfiguration to point to the new vSphere ESXI Dump server.
vSphere Update Manager	Not installed on the vCenter Server system	Relocated as part of the vCenter Server system or the vCenter Server Appliance	Run Migration Assistant on the source Update Manager machine, if Update Manager is installed on an different machine from vCenter Server.

For more information about upgrade scenarios, see Example Upgrade Paths for vCenter Server version 5.5 to version 6.5.

For more information about migration scenarios, see Example Migration Paths from vCenter Server for Windows to vCenter Server Appliance 6.5.

When migrating vCenter Server instances to vCenter Server Appliance instances, some services do not behave the same way for vCenter Server for Windows and vCenter Server Appliance. For details on services that differ between vCenter Server for Windows and vCenter Server Appliance, see Differences between Upgrading and Migrating vCenter Server on Windows.

Differences between Upgrading and Migrating vCenter Server on Windows

You have two choices for moving your vCenter Server deployment on Windows to version 6.5: you can use the upgrade on Windows process or you can use the migration process to convert your deployment to an appliance at the same time that you upgrade the deployment to version 6.5.

It is important to understand the differences and similarities between upgrading and migrating vCenter Server instances on Windows.

- Choose the upgrade on Windows process to upgrade a vCenter Server version 5.5 or version 6.0 deployment on Windows to a vCenter Server 6.5 deployment on Windows. For details, see Chapter 3 Upgrading vCenter Server for Windows.
- Choose the migration to an appliance process to convert a vCenter Server version 5.5 or version 6.0 deployment on Windows to a vCenter Server Appliance 6.5 deployment. For details, see Chapter 4 Migrating vCenter Server for Windows to vCenter Server Appliance .

You can migrate the following vCenter Server deployment types from Windows to appliances while upgrading to version 6.5:

- vCenter Server with an embedded vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0)
- vCenter Server with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0)

You can migrate with an embedded or external vCenter database. In either case, the database is converted to an embedded PostgreSQL database on the new appliance. For more about the database migration, see Preparing vCenter Server Databases for Migration.

You can migrate a vCenter Server installation to an appliance using either the GUI method or CLI method.

- When migrating vCenter Server with an embedded vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0), the migration is a single workflow.
- When migrating vCenter Server with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0), migration order matters. You migrate vCenter Single Sign-On (version 5.5) instances or Platform Services Controller instances before migrating vCenter Server instances. For details, see Chapter 4 Migrating vCenter Server for Windows to vCenter Server Appliance .

Preparation includes using VMware Migration Assistant to gather the required information on the source vCenter Server instance, vCenter Single Sign-On instance, or Platform Services Controller instance. For details, see Download and Run VMware Migration Assistant on the Source Windows Machine.

Upgrading or Migrating to vSphere License Service

The License Service is 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, vSAN clusters, and other products that you use with vSphere.

After the upgrade or migration 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, Patches, Updates, and Migrations

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

VMware product versions are numbered with two digits, for example, vSphere 6.5. A release that changes either digit, for example, from 5.5 to 6.0, or from 6.0 to 6.5, involves major changes in the software, and requires an upgrade from the previous version. A release that makes a smaller change, requiring only a patch or update, is indicated by an update number, for example, vSphere 6.0 Update 1.

For information about upgrading vCenter Server installations, see Chapter 2 Upgrading the vCenter Server Appliance and Platform Services Controller Appliance or Chapter 3 Upgrading vCenter Server for Windows.

For information about patching or updating vCenter Server, see Chapter 7 Patching and Updating vCenter Server 6.5 Deployments

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

When you upgrade a vCenter Server for Windows instance and at the same time convert it to a vCenter Server Appliance instance, it is a migration.

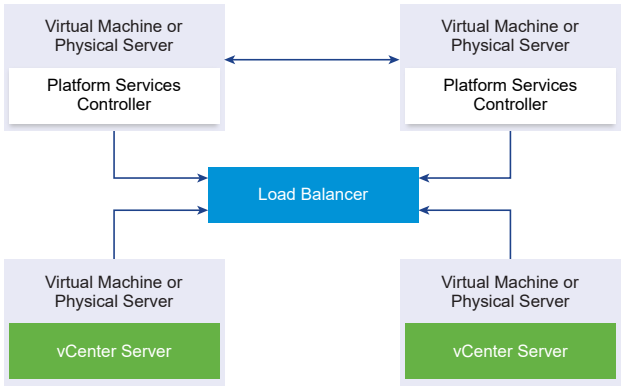
For information about migrating a vCenter Server installation to an appliance, see Chapter 4 Migrating vCenter Server for Windows to vCenter Server Appliance .

Deployment Topologies with External Platform Services Controller Instances and High Availability

To ensure Platform Services Controller high availability in external deployments, you must install or deploy at least two joined Platform Services Controller instances in your vCenter Single Sign-On domain. When you use a third-party load balancer, you can ensure an automatic failover without downtime.

Platform Services Controller with a Load Balancer

Figure 1-17. Example of a Load Balanced Pair of Platform Services Controller Instances



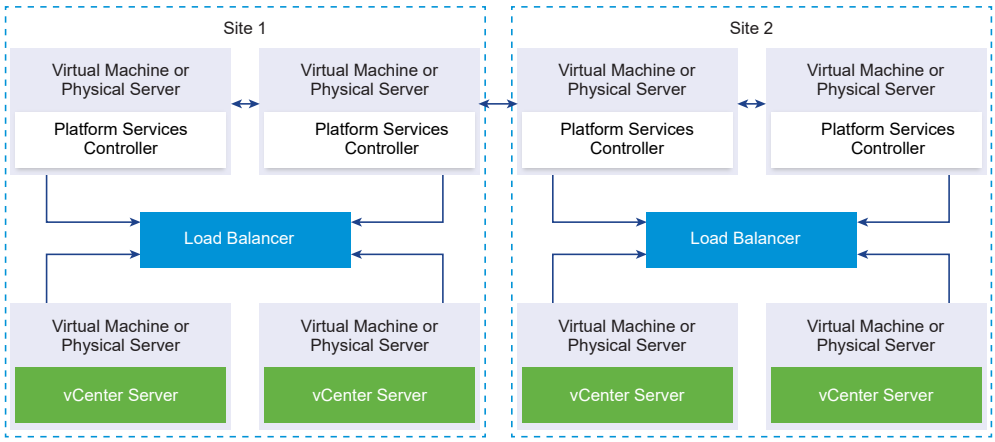
You can use a third-party load balancer per site to configure Platform Services Controller high availability with automatic failover for this site. For information about the maximum number of Platform Services Controller instances behind a load balancer, see the *Configuration Maximums* documentation.

Important To configure Platform Services Controller high availability behind a load balancer, the Platform Services Controller instances must be of the same operating system type. Mixed operating systems Platform Services Controller instances behind a load balancer are unsupported.

The vCenter Server instances are connected to the load balancer. When a Platform Services Controller instance stops responding, the load balancer automatically distributes the load among the other functional Platform Services Controller instances without downtime.

Platform Services Controller with Load Balancers Across vCenter Single Sign-On Sites

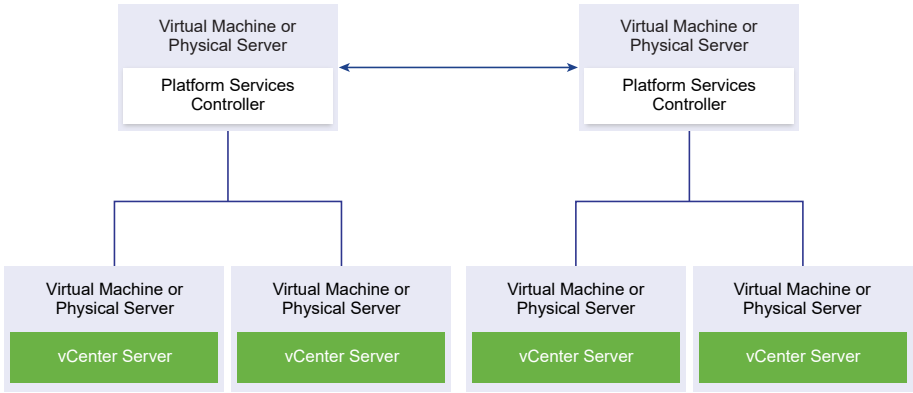
Figure 1-18. Example of Two Load Balanced Pairs of Platform Services Controller Instances Across Two Sites



Your vCenter Single Sign-On domain might span multiple sites. To ensure Platform Services Controller high availability with automatic failover throughout the domain, you must configure a separate load balancer in each site.

Platform Services Controller with No Load Balancer

Figure 1-19. Example of Two Joined Platform Services Controller Instances with No a Load Balancer

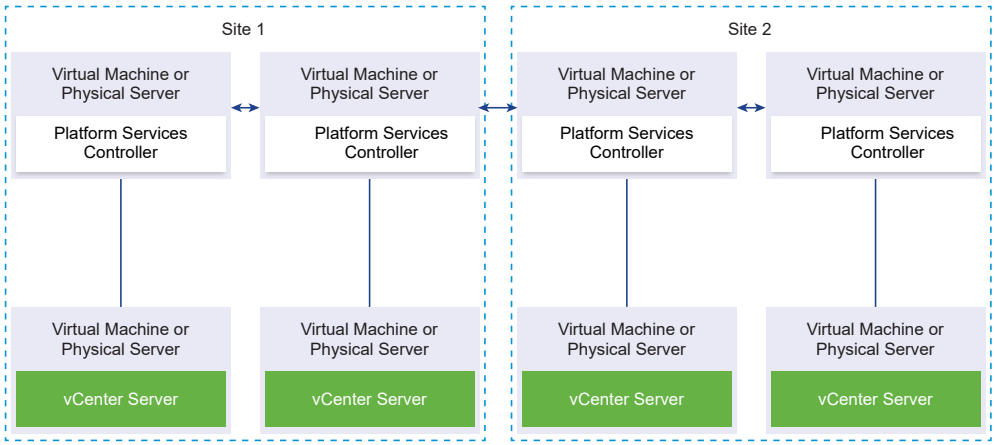


When you join two or more Platform Services Controller instances in the same site with no load balancer, you configure Platform Services Controller high availability with a manual failover for this site.

Note If your vCenter Single Sign-On domain includes three or more Platform Services Controller instances, you can manually create a ring topology. A ring topology ensures Platform Services Controller reliability when one of the instances fails. To create a ring topology, run the `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` command against the first and last Platform Services Controller instance that you have deployed.

Platform Services Controller with No Load Balancer Across vCenter Single Sign-On Sites

Figure 1-20. Example of Two Joined Pairs of Platform Services Controller Instances Across Two Sites with No Load Balancer



Important Repointing vCenter Server between sites and domains is unsupported. If no functional Platform Services Controller instance is available in the site, you must deploy or install a new Platform Services Controller instance in this site. This new Platform Services Controller instance becomes the replication partner of the existing Platform Services Controller instance.

Moving from a Deprecated to a Supported vCenter Server Deployment Topology Before Upgrade or Migration

Before you upgrade or migrate your environment to vSphere 6.5, you must move any deprecated deployment topology to a supported deployment topology.

When you first install vCenter Server 5.5 or 6.0, you deployment includes either an embedded Platform Services Controller or vCenter Single Single-On, or an external Platform Services Controller or vCenter Single Single-On.

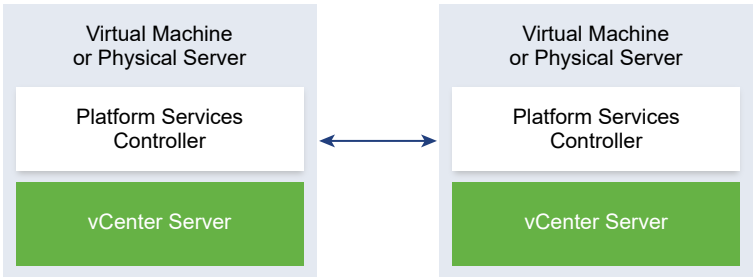
If you upgrade or migrate your deployment later you have two options:

- Join a vCenter Server with an external Platform Services Controller to a Platform Services Controller.
- Join an external Platform Services Controller to a Platform Services Controller.

The installer does not validate whether the Platform Services Controller is external or embedded with vCenter Server. Although many types of join operations are possible, not all resulting topologies are supported. Before you upgrade or migrate your environment to vSphere 6.5, you must move any deprecated deployment topology to a supported deployment topology.

Moving to a Supported Topology from vCenter Server instances with Embedded Platform Services Controller or vCenter Single Single-On in Replication

Figure 1-21. Deprecated Topology of vCenter Server instances with Embedded Platform Services Controller or vCenter Single Single-On in Replication

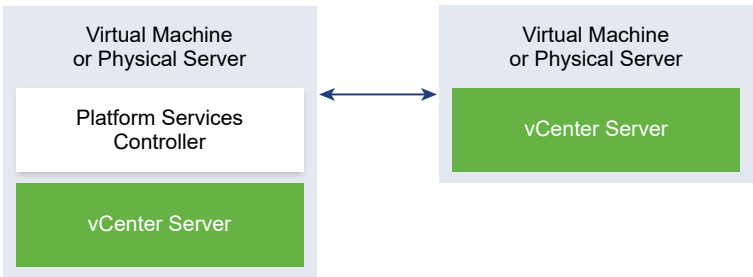


To move a vSphere 5.5 deployment to a supported topology, follow the instructions in http://kb.vmware.com /kb/2130433.

To move a vSphere 6.0 deployment to a supported topology, see the instructions on repointing the connections between vCenter Server and Platform Services Controller in the *vSphere Upgrade* 6.0 documentation.

Moving to a Supported Topology from a vCenter Server Pointing to an Embedded Platform Services Controller

Figure 1-22. Deprecated topology of a vCenter Server Pointing to an Embedded Platform Services Controller

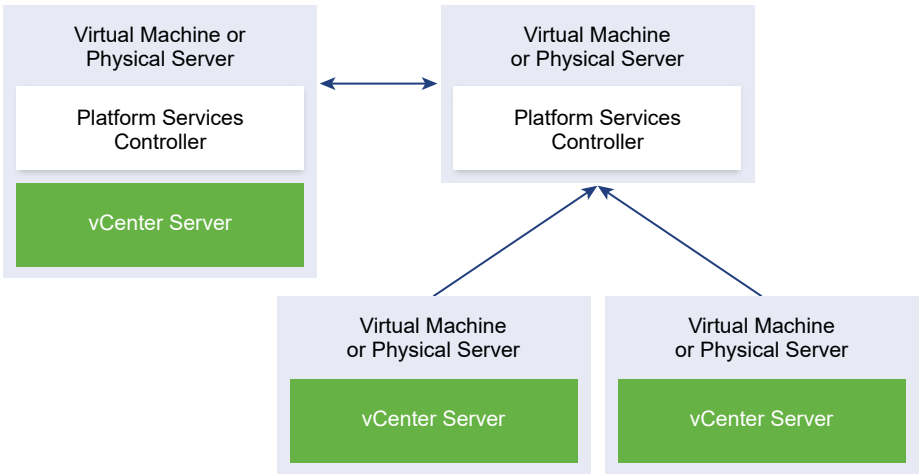


To move a vSphere 5.5 deployment to a supported topology, follow the instructions in http://kb.vmware.com/kb/2128430.

To move a vSphere 6.0 deployment to a supported topology, see the instructions on repointing the connections between vCenter Server and Platform Services Controller in the *vSphere Upgrade* 6.0 documentation.

Moving to a Supported Topology from an Embedded Platform Services Controller and an External Platform Services Controller in Replication

Figure 1-23. Deprecated Topology of an Embedded Platform Services Controller and an External Platform Services Controller in Replication



To move a vSphere 5.5 deployment to a supported topology, follow the instructions in http://kb.vmware.com/kb/2130436.

To move a vSphere 6.0 deployment to a supported topology, see the instructions on repointing the connections between vCenter Server and Platform Services Controller in the *vSphere Upgrade* 6.0 documentation.

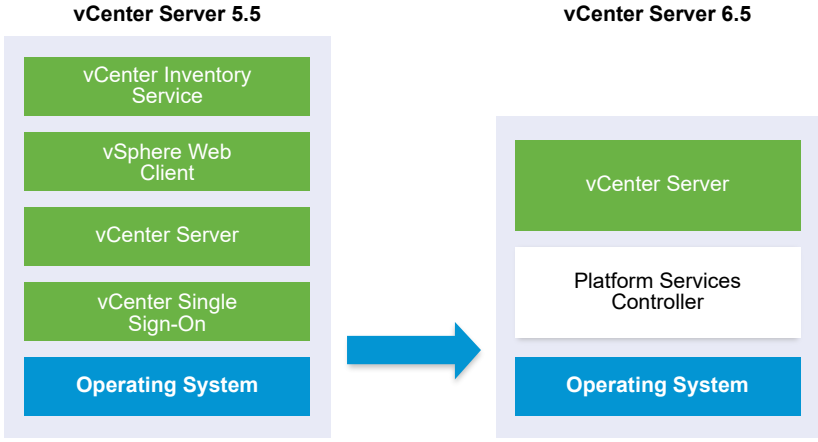
Example Upgrade Paths for vCenter Server version 5.5 to version 6.5

Your initial vCenter Server 5.5 configuration determines your upgrade and configuration options.

The vCenter Server 5.5 example upgrade paths demonstrate some common starting configurations before vCenter Server upgrade and their expected configuration outcomes after vCenter Server upgrade.

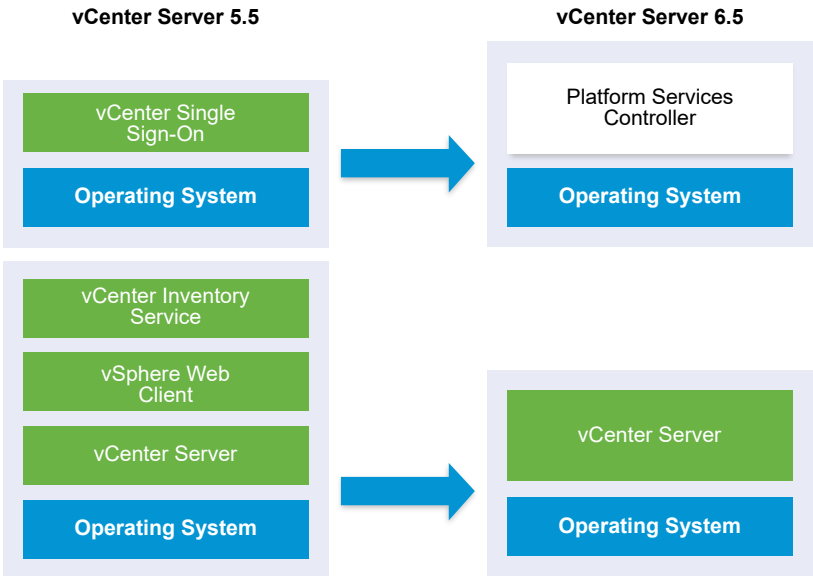
If you have a simple installation with all vCenter Server 5.5 components on the same system, the vCenter Server 6.5 software upgrades your system to vCenter Server with an embedded Platform Services Controller instance. The software upgrades your vCenter Server common services such as vCenter Single 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 6.5 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 1-24. vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Upgrade



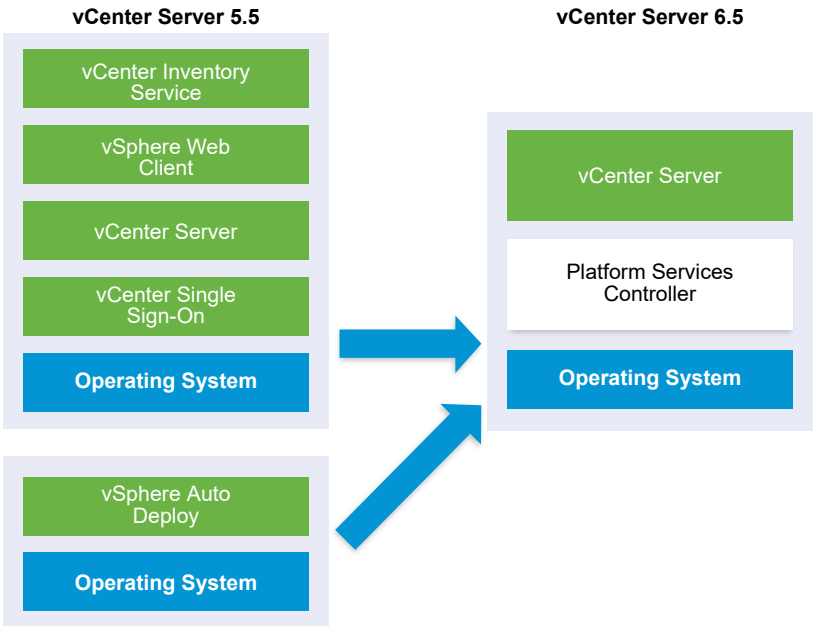
If you have a custom vCenter Server 5.5 environment with an externally deployed vCenter Single Sign-On, the vCenter Server 6.5 software upgrades your deployment to vCenter Server with an external Platform Services Controller instance.

Figure 1-25. vCenter Server 5.5 with External 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 6.5. 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.

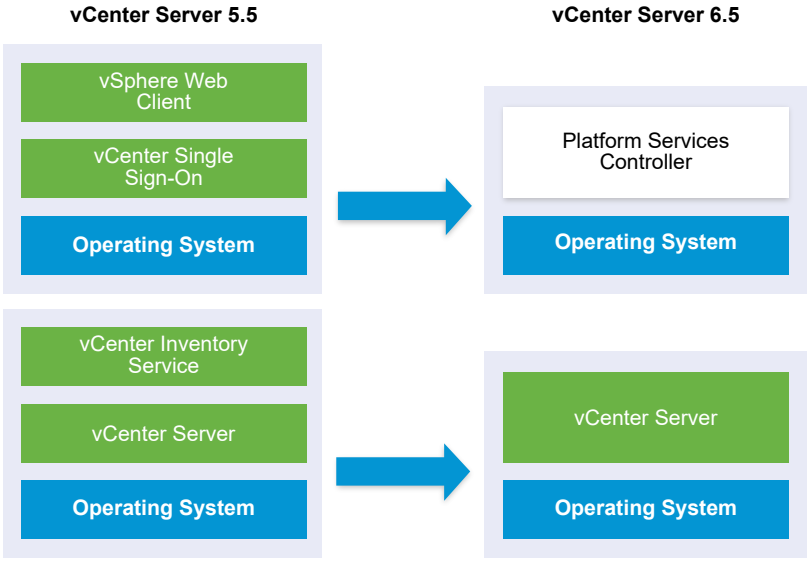
Figure 1-26. vCenter Server 5.5 with Remote vSphere Auto Deploy Server Before and After Upgrade



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.

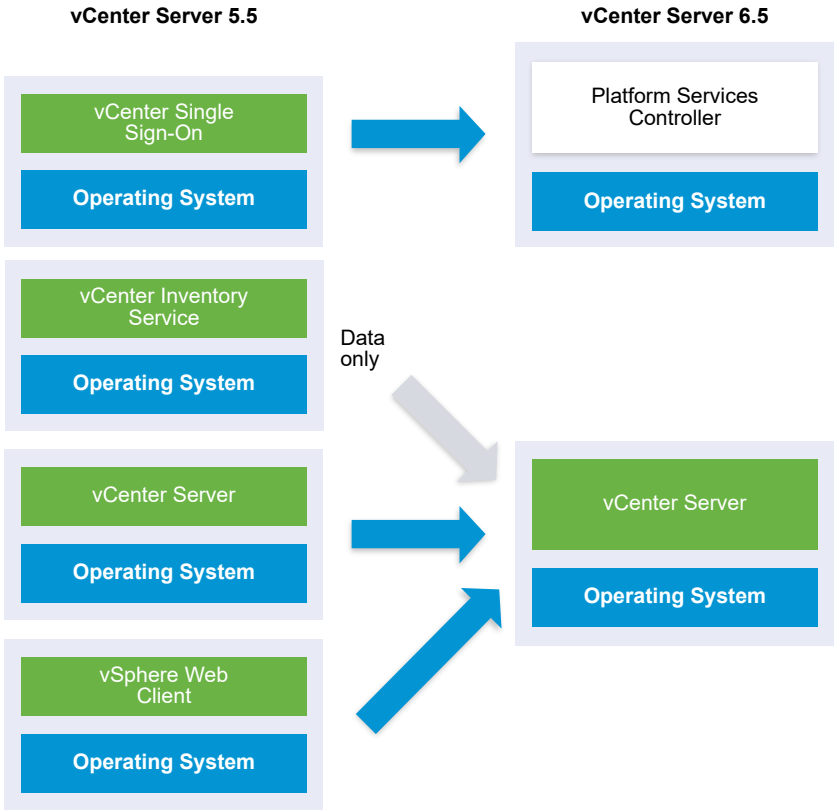
If your configuration includes a remotely deployed vSphere Web Client, it is upgraded along with the vCenter Server instance to which it is registered and migrated to the same location as the vCenter Server instance.

Figure 1-27. vCenter Server 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 6.5. 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 Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration

Figure 1-28. vCenter Server 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.

For more information on mixed version transitional environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

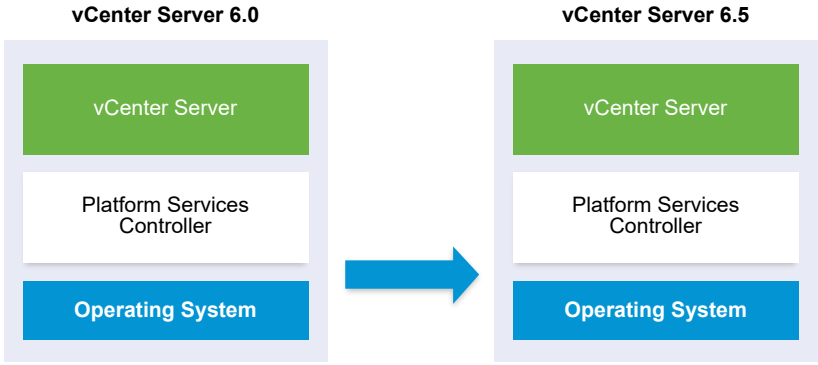
Example Upgrade Paths from vCenter Server version 6.0.x to version 6.5

Your vCenter Server 6.0 deployment type does not change during the upgrade to version 6.5.

The vCenter Server example upgrade paths demonstrate vCenter Server 6.0 upgrade outcomes.

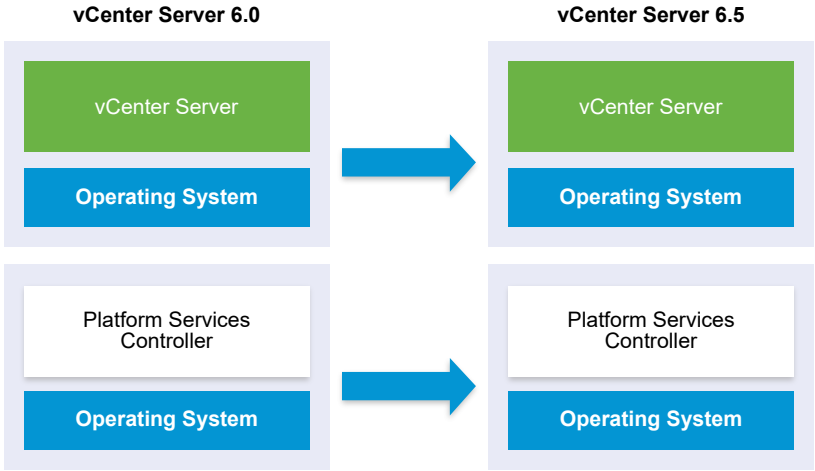
The installer upgrades vCenter Server 6.0.x with an embedded Platform Services Controller instance to vCenter Server 6.5 with an embedded Platform Services Controller instance. The software upgrades vCenter Server and Platform Services Controller instance in the correct order to the same version.

Figure 1-29. vCenter Server 6.0.x with Embedded Platform Services Controller Before and After Upgrade



The installer upgrades an external vCenter Server 6.0.x instance to an external vCenter Server 6.5 instance and an external Platform Services Controller 6.0.x instance to an external Platform Services Controller 6.5 instance.

Figure 1-30. vCenter Server 6.0.x with External Platform Services Controller 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 multi-site 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.

For more information on mixed version transitional environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Example Migration Paths from vCenter Server for Windows to vCenter Server Appliance 6.5

You can migrate a vCenter Server for Windows instance to a vCenter Server Appliance instance.

You can migrate a vCenter Server version 5.5 or version 6.0 instance on Windows to a vCenter Server Appliance 6.5 deployment on a Linux-based OS.

The vCenter Server example migration paths demonstrate supported migration outcomes.

You can migrate a vCenter Server instance with an embedded vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.5 instance with an embedded Platform Services Controller appliance. In this case the software migrates the vCenter Server instance and the embedded vCenter Single Sign-On instance or Platform Services Controller instance at the same time.

Figure 1-31. vCenter Server 5.5.x with Embedded vCenter Single Sign-On Installation Before and After Migration

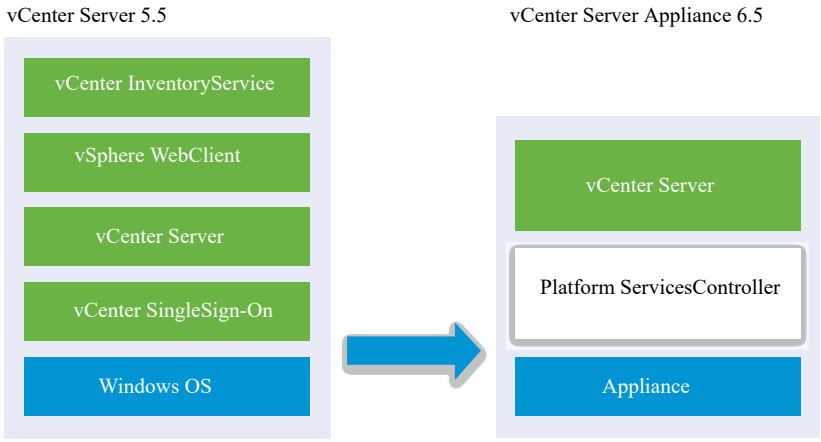
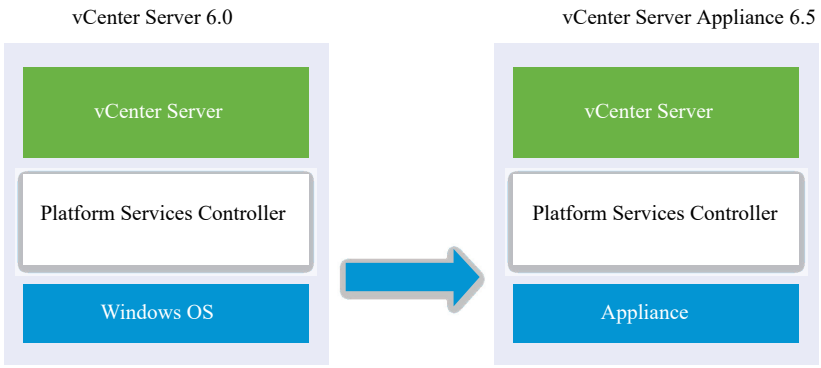


Figure 1-32. vCenter Server 6.0.x with Embedded Platform Services Controller Installation Before and After Migration



You can migrate a vCenter Server instance with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.5 instance with an external Platform Services Controller appliance. In this case you must first migrate the external vCenter Single Sign-On instance or Platform Services Controller instance and then the vCenter Server instance.

Figure 1-33. vCenter Server 5.5.x with External vCenter Single Sign-On Installation Before and After Migration

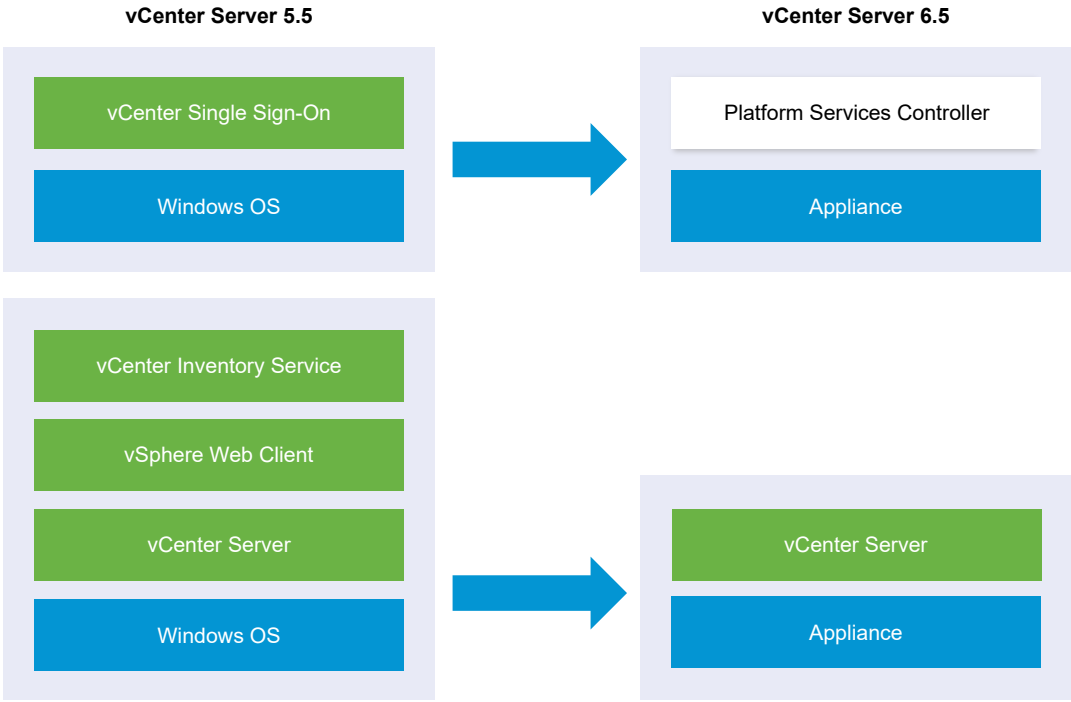
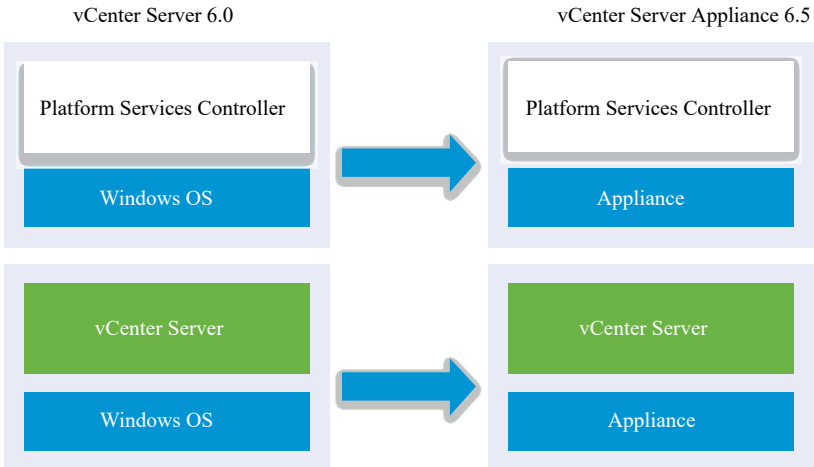


Figure 1-34. vCenter Server 6.0.x with External Platform Services Controller Installation Before and After Migration



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 multi-site 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.

For more information on mixed version transitional environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Upgrading the vCenter Server Appliance and Platform Services Controller Appliance

2

You can upgrade the vCenter Server Appliance 5.5 or 6.0 and the Platform Services Controller appliance 6.0 to version 6.5. All of the installation files that are necessary for the upgrade are included in the vCenter Server Appliance installer, which you can download from the VMware Web site.

The upgrade of the vCenter Server Appliance or Platform Services Controller appliance is a migration of the old version to the new version, which includes deploying a new appliance of version 6.5. You can deploy the new appliance on an ESXi host 5.5 or later, or on the inventory of a vCenter Server instance 5.5 or later. You assign a temporary IP address to the new appliance to facilitate the configuration and services data migration from the old appliance to the newly deployed appliance. After the migration, the IP address and host name of the old appliance are applied to the new upgraded appliance of version 6.5. At the end of the upgrade, the temporary IP address is released and the old appliance is powered off.

Version 6.5 of the vCenter Server Appliance uses the embedded PostgreSQL database. If you are upgrading a vCenter Server Appliance that is using an external database, the external database will be migrated to the embedded PostgreSQL database of the new upgraded appliance. During the upgrade, you must select a storage size for the new appliance that is suitable for the database size.

Version 6.5 of the vCenter Server Appliance uses the embedded VMware vSphere Update Manager Extension service. If you are upgrading a vCenter Server Appliance that is using an external VMware Update Manager instance, the external VMware Update Manager instance will be migrated to the embedded VMware vSphere Update Manager Extension of the new upgraded appliance. The embedded VMware vSphere Update Manager Extension uses the embedded PostgreSQL database. Before the upgrade, you must run the Migration Assistant on the source VMware Update Manager instance.

For information about the software included in the vCenter Server Appliance 6.5, see *vSphere Installation and Setup*.

Important For topologies with external Platform Services Controller instances, you must upgrade the replicating Platform Services Controller instances in a sequence. After the successful upgrade of all Platform Services Controller instances in the domain, you can perform concurrent upgrades of multiple vCenter Server appliances that point to a common external Platform Services Controller instance.

The vCenter Server Appliance installer contains executable files GUI and CLI upgrades which you can use alternatively.

- The GUI upgrade is a two stage process. The first stage is a deployment wizard that deploys the OVA file of the new appliance on the target ESXi host or vCenter Server instance. After the OVA deployment finishes, you are redirected to the second stage of the process that sets up and transfers the services and configuration data from the old appliance to the newly deployed appliance.
- The CLI upgrade method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that automatically deploys the new appliance and transfers the services and configuration data from the old appliance.

For information about the vCenter Server Appliance and Platform Services Controller appliance upgrade requirements, see System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance.

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

If the 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.

To upgrade a vCenter Server Appliance 5.0 or 5.1, you must first upgrade to version 5.5 or 6.0 and then upgrade to version 6.5. For information about upgrading the vCenter Server Appliance 5.0 or 5.1 to version 5.5, see the *VMware vSphere 5.5 Documentation*. For information about upgrading the vCenter Server Appliance 5.1 Update 3 to version 6.0, see the *VMware vSphere 6.0 Documentation*.

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

For information about configuring the vCenter Server Appliance, see *vCenter Server Appliance Configuration*.

This chapter includes the following topics:

- CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance

About the Upgrade Process of the vCenter Server Appliance and Platform Services Controller Appliance

You can upgrade the vCenter Server Appliance from version 5.5 or 6.0 to version 6.5. You can upgrade the Platform Services Controller appliance from version 6.0 to version 6.5.

When you run the GUI or CLI upgrade, the process includes:

1 Deploying a new appliance of version 6.5 with temporary network configuration

   If you are upgrading a vCenter Server Appliance, you must select a deployment size for the new appliance that is suitable for your vSphere environment size. You must also select a storage size for the new appliance that is suitable for the vCenter Server Appliance database. If the source vCenter Server Appliance uses an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance.

2 Exporting the services and configuration data from the source appliance of version 5.5.x or 6.0.x. that you want to upgrade

   You must select the data types that you want to transfer to the new appliance.

   If you are upgrading a vCenter Server Appliance that uses an external Update Manager instance, you must ensure that the Migration Assistant is running on the Update Manager machine, which facilitates the export of the Update Manager configuration and database.

3 Transferring the exported data to the newly deployed appliance

   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.

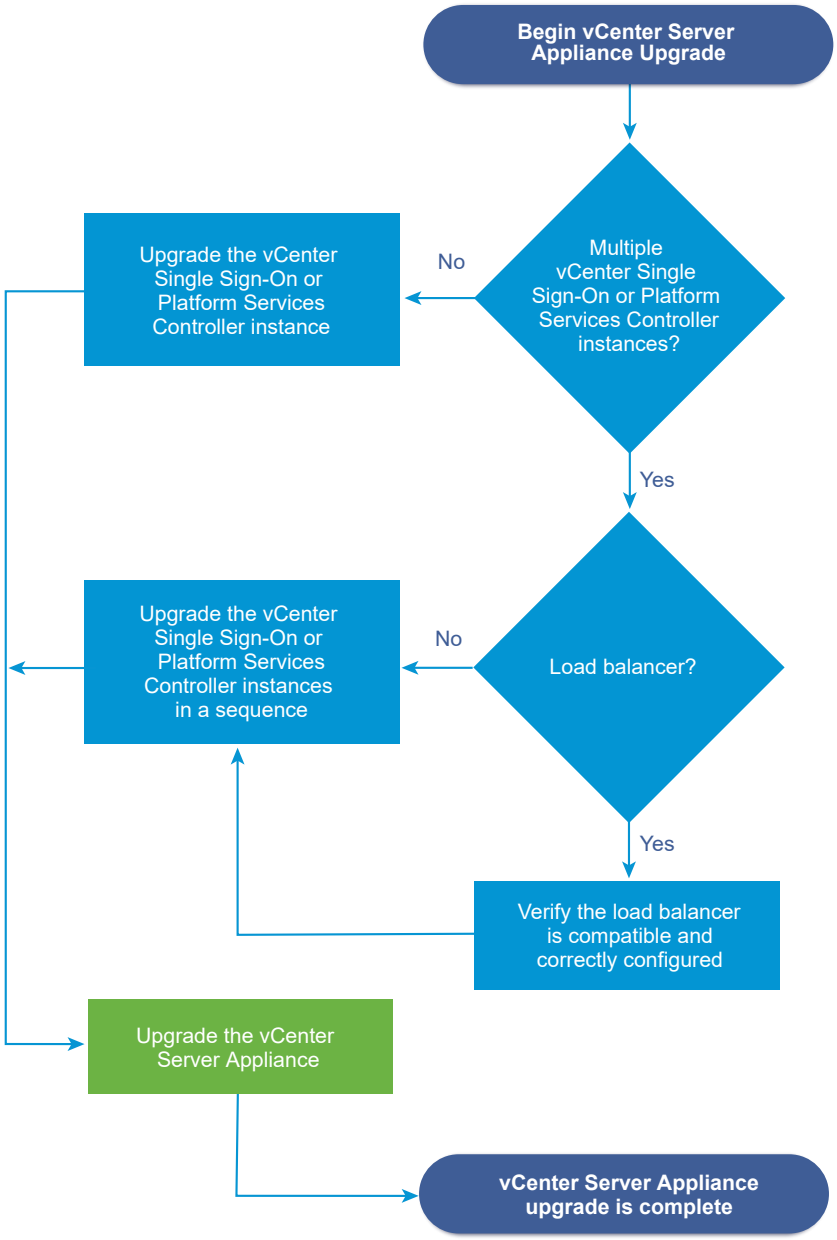
   If the source vCenter Server Appliance uses an external database, the database is migrated to the embedded PostgreSQL database of the new appliance.

   If you are upgrading a vCenter Server Appliance that uses a Update Manager instance, the Update Manager instance is migrated to the embedded VMware vSphere Update Manager Extension of the new upgraded appliance.

4 Powering off the source appliance. The new upgraded appliance assumes the network configuration of the source appliance.

If your current appliance version is earlier than 5.5, you must upgrade to 5.5 or 6.0 before upgrading to version 6.5.

Figure 2-1. Upgrade Workflow for a vCenter Server Appliance with an External Platform Services Controller



- For the new appliance requirements, see System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance.
- For the appliance upgrade preparation, see Preparing to Upgrade the vCenter Server Appliance and Platform Services Controller Appliance.
- For the appliance upgrade procedures, see Chapter 2 Upgrading the vCenter Server Appliance and Platform Services Controller Appliance.
- For the appliance post-upgrade procedures, see Chapter 5 After Upgrading or Migrating vCenter Server.

System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance

The upgrade of the appliance is a migration of the old version to the new version, which includes deploying a new appliance of version 6.5. You can deploy the new vCenter Server Appliance or Platform Services Controller appliance on an ESXi host 5.5 or later, or on a vCenter Server instance 5.5 or later. Your system must also meet specific software and hardware requirements.

When you use Fully Qualified Domain Names, verify that the client machine from which you are deploying the appliance and the network on which you are deploying the appliance use the same DNS server.

Before you deploy the new appliance, synchronize the clocks of the target server and all vCenter Server and Platform Services Controller instances on the vSphere network. Unsynchronized clocks might result in authentication problems and can cause the installation to fail or prevent the appliance services from starting. See Synchronizing Clocks on the vSphere Network.

Hardware Requirements for the vCenter Server Appliance and Platform Services Controller Appliance

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 determines the number of CPUs and the amount of memory for the appliance. The size of the Platform Services Controller appliance is the same for all environment sizes.

Hardware Requirements for the vCenter Server Appliance

The hardware requirements for a vCenter Server Appliance depend on the size of your vSphere inventory.

Table 2-1. Hardware Requirements for a vCenter Server Appliance with an Embedded or External Platform Services Controller

	Number of vCPUs	Memory
Tiny environment (up to 10 hosts or 100 virtual machines)	2	10 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	4	16 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	8	24 GB

Table 2-1. Hardware Requirements for a vCenter Server Appliance with an Embedded or External Platform Services Controller (continued)

	Number of vCPUs	Memory
Large environment (up to 1,000 hosts or 10,000 virtual machines)	16	32 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	24	48 GB

Note If you want to add an ESXi host with more than 512 LUNs and 2,048 paths to the vCenter Server Appliance inventory, you must deploy a vCenter Server Appliance for a large or x-large environment.

Hardware Requirements for the Platform Services Controller Appliance

The hardware requirements for a Platform Services Controller appliance are 2 vCPUs and 4 GB memory.

Storage Requirements for the vCenter Server Appliance and Platform Services Controller Appliance

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

Storage Requirements for the vCenter Server Appliance

The storage requirements are different for each vSphere environment size and depend on your database size requirements.

Table 2-2. Storage Requirements for a vCenter Server Appliance with an Embedded or External Platform Services Controller

	Default Storage Size	Large Storage Size	X-Large Storage Size
Tiny environment (up to 10 hosts or 100 virtual machines)	250 GB	775 GB	1650 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	290 GB	820 GB	1700 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	425 GB	925 GB	1805 GB

Table 2-2. Storage Requirements for a vCenter Server Appliance with an Embedded or External Platform Services Controller (continued)

	Default Storage Size	Large Storage Size	X-Large Storage Size
Large environment (up to 1,000 hosts or 10,000 virtual machines)	640 GB	990 GB	1870 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	980 GB	1030 GB	1910 GB

Note The storage requirements include the requirements for the VMware Update Manager that runs as a service in the vCenter Server Appliance.

Storage Requirements for the Platform Services Controller Appliance

The storage requirement for a Platform Services Controller appliance is 60 GB.

Software Requirements for the vCenter Server Appliance and Platform Services Controller Appliance

The VMware vCenter Server Appliance and Platform Services Controller appliance can be deployed on ESXi hosts 5.5 or later, or on vCenter Server instances 5.5 or later.

You can deploy the vCenter Server Appliance or Platform Services Controller appliance by using the GUI or CLI installer. You run the installer from a network client machine that you use to connect to the target server and deploy the appliance on the server. You can connect directly to an ESXi 5.5.x or 6.x host on which to deploy the appliance. You can also connect to a vCenter Server 5.5.x or 6.x instance to deploy the appliance on an ESXi host or DRS cluster that resides in the vCenter Server inventory.

For information about the requirements for network client machine, see System Requirements for the vCenter Server Appliance Installer.

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.

vCenter Server is accessed through 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. For the list of all supported ports and protocols in vCenter Server, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/.

During installation, if a port is in use or is blocked using a denylist, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation.

VMware uses designated ports for communication. Also, the managed hosts monitor designated ports for data from vCenter Server. If a built-in 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.

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.

DNS Requirements for the vCenter Server Appliance and Platform Services Controller Appliance

When you deploy the new vCenter Server Appliance or Platform Services Controller appliance, in the temporary network settings, you can assign a static IP address and an FQDN that is resolvable by a DNS server. After the upgrade, the appliance frees this static IP address and assumes the network settings of the old appliance.

When you deploy the vCenter Server Appliance or Platform Services Controller appliance with a static IP address, you ensure that in case of system restart, the IP address of the appliance remains the same.

Before you deploy the vCenter Server Appliance or Platform Services Controller appliance with a static IP address, you must verify that this IP address has a valid internal domain name system (DNS) registration.

When you deploy the vCenter Server Appliance, 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 (FQDN) for the appliance from its IP address. Reverse lookup is implemented using PTR records.

If you plan to use an FQDN for the appliance system name, you must verify that the FQDN is resolvable by a DNS server.

You can use the `nslookup` command to verify that the DNS reverse lookup service returns an FQDN when queried with the IP address and to verify that the FQDN is resolvable.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

If you use DHCP instead of a static IP address for the vCenter Server Appliance or Platform Services Controller appliance, verify that the appliance name is updated in the domain name service (DNS). If you can ping the appliance 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 6.5 requires Adobe Flash Player v. 16 to 23. For best performance and security fixes, use Adobe Flash Player 23.

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 2-3. Supported Guest Operating Systems and Minimum Browser Versions for the vSphere Web Client

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Edge v. 79 to 86. Mozilla Firefox v. 60 to 84. Google Chrome v. 75 to 86.
Mac OS	Microsoft Edge v. 79 to 86. Mozilla Firefox v. 60 to 84. Google Chrome v. 75 to 86.

Preparing to Upgrade the vCenter Server Appliance and Platform Services Controller Appliance

Before you upgrade the vCenter Server Appliance or Platform Services Controller appliance, you must download the vCenter Server Appliance installer ISO file and mount it to a network virtual machine or physical server from which you want to perform the upgrade.

The machine from which you upgrade the appliance must run on a Windows, Linux, or Mac operating system that meets the operating system requirements. See System Requirements for the vCenter Server Appliance Installer.

Before upgrading a vCenter Server Appliance, you must prepare the ESXi hosts in the inventory.

If the vCenter Server Appliance uses an external Oracle database, you must determine the size of the existing database.

If vCenter Server Appliance uses an external Update Manager instance, you must run the Migration Assistant on the Update Manager machine.

System Requirements for the vCenter Server Appliance Installer

You can run the vCenter Server Appliance GUI or CLI installer from a network client machine that is running on a Windows, Linux, or Mac operating system of a supported version.

To ensure optimal performance of the GUI and CLI installers, use a client machine that meets the minimum hardware requirements.

Table 2-4. System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	■ Windows 7, 8, 8.1, 10 ■ Windows 2012 x64 bit ■ Windows 2012 R2 x64 bit ■ Windows 2016 x64 bit	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	■ SUSE 12 ■ Ubuntu 14.04	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC **Note** The CLI installer requires 64-bit OS.
Mac	■ macOS v10.9, 10,10, 10.11 ■ macOS Sierra	8 GB RAM, 1 CPU having 4 cores with 2.4 GHz, 150 GB hard disk, 1 NIC

Note For client machines that run on Mac 10.11, concurrent GUI deployments of multiple appliances are unsupported. You must deploy the appliances in a sequence.

Download and Mount the vCenter Server Appliance Installer

VMware releases the vCenter Server Appliance ISO image, which contains GUI and CLI installers for the vCenter Server Appliance and Platform Services Controller appliance.

With the GUI and CLI executable files that are included in the vCenter Server Appliance installer, you can:

- Deploy the vCenter Server Appliance and Platform Services Controller appliance.
- Upgrade the vCenter Server Appliance and Platform Services Controller appliance.
- Migrate Windows installations of vCenter Server, vCenter Single Sign-On, and Platform Services Controller to the vCenter Server Appliance and Platform Services Controller appliance.
- Restore a vCenter Server Appliance from a file-based backup.

Prerequisites

- Create a Customer Connect account at https://my.vmware.com/web/vmware/.
- Verify that your client machine meets the system requirements for the vCenter Server Appliance installer. See System Requirements for the vCenter Server Appliance Installer.

Procedure

1. Log in to VMware Customer Connect.
2. Navigate to **Products and Accounts > All Products**.
3. Find VMware vSphere and click **View Download Components**.

4 Select a VMware vSphere version from the **Select Version** drop-down.

5 Select a version of VMware vCenter Server and click **GO TO DOWNLOADS**.

6 Download the vCenter Server appliance ISO image.

7 Confirm that the md5sum is correct by using an MD5 checksum tool.

8 Mount or extract the ISO image to the client machine from which you want to deploy, upgrade, migrate, or restore the appliance.

Note ISO mounting or extracting software that does not allow more than eight directory levels is unsupported.

For example, MagicISO Maker is unsupported on Windows. For Linux OS and Mac OS, Archive Manager is unsupported.

For Mac OS, you can use DiskImageMounter.
For Ubuntu 14.04, you can use Disk Image Mounter.
For SUSE 12 OS, you can use the terminal.

```
$ sudo mkdir mount_dir
$ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
```

What to do next

Open the `readme.txt` file and review the information about the other files and directories in the vCenter Server Appliance ISO image.

Synchronizing Clocks on the vSphere Network

Verify 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.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the Knowledge Base article http://kb.vmware.com/kb/1318.

To synchronize ESXi clocks with an NTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see *vSphere Single Host Management*.

Prepare ESXi Hosts for vCenter Server Appliance Upgrade

Before upgrading to vCenter Server Appliance 6.5, you must prepare your ESXi hosts.

Prerequisites

To upgrade vCenter Server Appliance, your ESXi hosts must meet the requirements for upgrade.

- ESXi hosts must be at version 5.5 or later. Read and follow all best practices when upgrading your hosts to ESXi 5.5.
- Your target host must be running ESXi 5.5 or later.
- Your source and target ESXi hosts must not be in lockdown or maintenance mode and not part of fully automated DRS clusters.

Procedure

1. To keep your current SSL certificates, back up the SSL certificates that are on the vCenter Server Appliance system before you upgrade to vCenter Server Appliance 6.5.

   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 Appliance 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 Appliance upgrade.

Host Upgrades and Certificates

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

If you decide not to upgrade your hosts to ESXi 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.

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 those hosts to ESXi 6.0 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 during upgrade. Change the certificate mode to **Custom** to ensure that the certificates are not replaced accidentally during a certificate refresh later.

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.

Hosts Provisioned with Auto Deploy

Hosts that are being provisioned by Auto Deploy are always assigned new certificates when they are first booted with ESXi 6.0 or later 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

Use VMCA to provision the ESXi hosts in your environment unless corporate policy requires that you use custom certificates. To use custom certificates with a different root CA, you can edit the vCenter Server `vpxd.certmgmt.mode` advanced option. After the change, the hosts are no longer automatically provisioned with VMCA certificates when you refresh certificates. You are 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 **Configure**.
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.

Determine the Oracle Database Size and the Storage Size for the New Appliance

Before upgrading a vCenter Server Appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new appliance so that the embedded PostgreSQL database can successfully assume the data from the old database with enough free disk space after the upgrade.

You run scripts to determine the Oracle core table size, the events and tasks table size, and the statistics table size. The Oracle core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Oracle events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Oracle tables size.

During the upgrade of the appliance, you can select the types of data to transfer to the new appliance. For minimum upgrade time and storage requirement for the new appliance, you can select to transfer only the configuration data.

Prerequisites

You must have the vCenter Server database login credentials.

Procedure

1 Log in to a SQL*Plus session with the vCenter Server database user.

2 Determine the core table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
  FROM   user_segments s
  WHERE  (s.segment_name,s.segment_type)
                IN (SELECT seg_name, seg_type FROM
                          (SELECT t.table_name seg_name, t.table_name tname,
                            'TABLE' seg_type
                            FROM   user_tables t
                           UNION
                           SELECT i.index_name, i.table_name,
                           'INDEX'
                            FROM   user_indexes i
                          ) ti
                     WHERE  (ti.tname LIKE 'VPX_%'
                             OR ti.tname LIKE 'CL_%'
                             OR ti.tname LIKE 'VDC_%')
                         AND ti.tname NOT LIKE 'VPX_SAMPLE_TIME%'
                         AND ti.tname NOT LIKE 'VPX_HIST_STAT%'
                         AND ti.tname NOT LIKE 'VPX_TOPN%'
                         AND ti.tname NOT LIKE 'VPX_SDRS_STATS_VM%'
```

```
                        AND ti.tname NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
                        AND ti.tname NOT LIKE 'VPX_TASK%'
                        AND ti.tname NOT LIKE 'VPX_EVENT%'
                        AND ti.tname NOT LIKE 'VPX_PROPERTY_BULLETIN%');
```

The script returns the database storage size in MB.

3 Determine the events and tasks table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                  WHERE
                     ti.tname LIKE 'VPX_TASK%'
                  OR ti.tname LIKE 'VPX_EVENT%');
```

The script returns the events and tasks storage size in MB.

4 Determine the statistics table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                  WHERE
                     ti.tname LIKE 'VPX_SAMPLE_TIME%'
                  OR ti.tname LIKE 'VPX_TOPN%'
                  OR ti.tname LIKE 'VPX_TASK%'
                  OR ti.tname LIKE 'VPX_EVENT%'
                  OR ti.tname LIKE 'VPX_HIST_STAT%');
```

The script returns the statistics storage size in MB.

5 Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.

   a The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Oracle core table returned in Step 2.

   b The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Oracle events and tasks and statistics tables returned in Step 3 and Step 4.

   For example, if the Oracle core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Download and Run VMware Migration Assistant on the Source Update Manager Machine

During the upgrade of a vCenter Server Appliance that uses an external Update Manager, the Migration Assistant must be running on the source Update Manager machine. This procedure describes how to download and run the Migration Assistant manually before the upgrade.

The Migration Assistant facilitates the migration of the Update Manager server and database to the new upgraded vCenter Server Appliance. The Migration Assistant uses port 9123 by default. If port 9123 is used by another service on your Update Manager machine, the Migration Assistant automatically finds a different free port to use.

Alternatively, if you plan to upgrade the vCenter Server Appliance by using the CLI installer, you can add the `source.vum section` section and `run.migration.assistant` subsection to your JSON template. For information about the CLI upgrade configuration parameters, see Upgrade Configuration Parameters.

Prerequisites

- Download and Mount the vCenter Server Appliance Installer.
- Log in to the source Update Manager machine as an administrator.

Procedure

1 From the vCenter Server Appliance installer package, copy the `migration-assistant` directory to the source Update Manager machine.

2 From the `migration-assistant` directory, double-click `VMware-Migration-Assistant.exe` and the provide the vCenter Single Sign-On administrator password.

3 Leave the Migration Assistant window open until the upgrade of the vCenter Server Appliance finishes.

Results

When the pre-checks are finished and any errors are addressed, your source Update Manager system is ready for the upgrade.

Caution Closing the Migration Assistant window causes the upgrade process to stop.

Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance

To ensure successful upgrade of the vCenter Server Appliance or Platform Services Controller appliance, you must preform some required tasks and pre-checks before running the upgrade.

General Prerequisites

- Download and Mount the vCenter Server Appliance Installer.
- Verify that the clocks of all machines on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not part of a fully automated DRS cluster.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster is not fully automated.

Source System Prerequisites

- Verify that the appliance that you want to upgrade does not run on an ESXi host that is part of a fully automated DRS cluster.
- Verify that port 22 is open on the appliance that you want to upgrade. The upgrade process establishes an inbound SSH connection to download the exported data from source appliance.
- If you are upgrading a vCenter Server Appliance that is configured with an external Update Manager, run the Migration Assistant on the source Update Manager machine.

For GUI upgrade, you must run the Migration Assistant manually. See Download and Run VMware Migration Assistant on the Source Update Manager Machine.

For CLI upgrade, you can run the Migration assistant either manually or automatically. To run the Migration Assistant automatically, add the `source.vum section` section and `run.migration.assistant` subsection to your JSON template. See Upgrade Configuration Parameters.

- Verify that port 443 is open on the source ESXi host on which the appliance that you want to upgrade resides. The upgrade process establishes an HTTPS connection to the source ESXi host to verify that the source appliance is ready for upgrade and to set up an SSH connection between the new and the existing appliance.
- If you are upgrading version 5.5 of the vCenter Server Appliance and you have changed its host name, verify that the SSL certificate is configured correctly. For information about how to troubleshoot an error when you changed the vCenter Server Appliance 5.5 host name, see *vSphere Troubleshooting* in the *VMware vSphere 5.5 Documentation*.
- Verify that you have sufficient free disk space on the appliance that you want to upgrade so that you can accommodate the data for the upgrade.
- Create an image-based backup of the vCenter Server appliance you are upgrading as a precaution in case there is a failure during the upgrade process. If you are upgrading a vCenter Server appliance with an external Platform Services Controller, take a image-based backup of the Platform Services Controller appliance as well.

  Important To take a pre-upgrade image-based backup, power off all the vCenter Server and Platform Services Controller nodes in your environment, and take a backup of each node. After you have taken backups of all the nodes, you can restart them and proceed with the upgrade procedure.

  If the upgrade fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server and Platform Services Controller nodes from their respective backups. You must restore all the nodes in the environment from their backups. Failing to do so will cause the replication partners to be out of synchronization with the restored node.

  To learn about image-based back, see "Image-Based Backup and Restore of a vCenter Server Environment" in *vCenter Server Installation and Setup*.
- If you use an external database, determine the database size and the minimum storage size for the new appliance. See Determine the Oracle Database Size and the Storage Size for the New Appliance.
- If you use an external database, back up the vCenter Server Appliance database.

Network Prerequisites

- Verify that the new appliance can connect to the source ESXi host or vCenter Server instance on which resides the appliance that you want to upgrade.

- If you plan to assign a static IP address and an FQDN as a system name in the temporary network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you plan to assign a DHCP IP address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is in the same network as the ESXi host on which the existing vCenter Server Appliance runs.
- If you plan to assign a DHCP IPv4 address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is connected to at least one network that is associated with a port group which accepts MAC address changes. Consider the default security policy of a distributed virtual switch, which is to reject MAC address changes. For information about how to configure the security policy for a switch or port group, see *vSphere Networking*.

GUI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance

You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance or Platform Services Controller appliance.

When you perform the GUI upgrade, you download the vCenter Server Appliance installer on a network client machine, run the upgrade wizard from the client machine, and provide the inputs that are required for the deployment and setup of the new upgraded appliance.

Important For topologies with external Platform Services Controller instances, you must upgrade the replicating Platform Services Controller instances in a sequence. After the successful upgrade of all Platform Services Controller instances in the domain, you can perform concurrent upgrades of multiple vCenter Server appliances that point to a common external Platform Services Controller instance.

The GUI upgrade process includes a series of two stages.

Figure 2-2. Stage 1 - OVA Deployment

The first stage walks you through the deployment wizard to get the deployment type of the source appliance that you want to upgrade and configure the new appliance settings. During this stage, you deploy the new appliance with temporary network settings. This stage completes the deployment of the OVA file on the target server with the same deployment type as the source appliance and the appliance settings that you provide.

As an alternative to performing the first stage of the upgrade with the GUI installer, you can deploy the OVA file of the new vCenter Server Appliance or Platform Services Controller appliance by using the vSphere Web Client or VMware Host Client. To deploy the OVA file on an ESXi host or vCenter Server instance 5.5 or 6.0, you can also use the vSphere Client. After the OVA deployment, you must log in to the appliance management interface of the newly deployed appliance to proceed with the second stage of the upgrade process.

Figure 2-3. Stage 2 - Appliance Setup

The second stage walks you through the setup wizard to choose the data types to transfer from the old to the new appliance. The new appliance uses the temporary network settings until the data transfer finishes. After the data transfer finishes, the new appliance assumes the network settings of the old appliance. This stage completes the data transfer, starts the services of the new upgraded appliance, and powers off the old appliance.

As an alternative to performing the second stage of the upgrade with the GUI installer, you can log in to the Appliance Management Interface of the newly deployed appliance, https://*FQDN_or_IP_address*:5480.

Required Information for Upgrading a vCenter Server Appliance 5.5 or 6.0 or Platform Services Controller Appliance 6.0

The GUI upgrade wizard prompts you for information about the vCenter Server Appliance 5.5, vCenter Server Appliance 6.0, or Platform Services Controller appliance 6.0 that you want to upgrade, deployment information for the new 6.5 appliance, and the types of data that you want to transfer from the old to the new appliance. It is a best practice to keep a record of the values that you entered.

You can use this worksheet to record the information that you need for upgrading a vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On, a vCenter Server Appliance 5.5 with an external vCenter Single Sign-On, a vCenter Server Appliance 6.0 with an embedded Platform Services Controller, a vCenter Server Appliance 6.0 with an external Platform Services Controller, or a Platform Services Controller appliance 6.0.

Table 2-5. Required Information During Stage 1 of the Upgrade

Required for Upgrade of	Required Information	Default	Your Entry
All deployment types	FQDN or IP address of the source appliance that you want to upgrade	-	
	HTTPS port of the source appliance	443	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
	vCenter Single Sign-On administrator user name of the source appliance **Important** The user must be administrator@*your_domain_name*.	administrator@vsphere.local	
	Password of the vCenter Single Sign-On administrator user	-	
	Password of the root user of the source appliance	-	
All deployment types	FQDN or IP address of the source server on which resides that appliance that you want to upgrade The source server can be either an ESXi host or a vCenter Server instance. **Note** The source server cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use the source ESXi host.	-	
	HTTPS port of the source server	443	
	User name with administrative privileges on the source server ■ If your source server is an ESXi host, use root. ■ If your source server is a vCenter Server instance, use *user_name@your_domain_name*, for example, administrator@vsphere.local.	-	
	Password of the user with administrative privileges on the source server	-	
All deployment types	FQDN or IP address of the target server on which you want to deploy the new appliance. The target server can be either an ESXi host or a vCenter Server instance. **Note** The target server cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	-	
	HTTPS port of the target server	443	
	User name with administrative privileges on the target server ■ If your target server is an ESXi host, use root. ■ If your target server is a vCenter Server instance, use *user_name@your_domain_name*, for example, administrator@vsphere.local.	-	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
	Password of the user with administrative privileges on the target server	-	
All deployment types Only if your target server is a vCenter Server instance	Data center from the vCenter Server inventory on which you want to deploy the new appliance Optionally you can provide a data center folder.	-	
	ESXi host or DRS cluster from the data center inventory on which you want to deploy the new appliance	-	
All deployment types	VM name for the new appliance ■ Must not contain a percent sign (%), backslash (\), or forward slash (/) ■ Must be no more than 80 characters in length	VMware vCenter Server Appliance	
All deployment types	Password for the root user of the appliance operating system ■ Must contain only lower ASCII characters without spaces. ■ Must be at least 8 characters, but no more than 20 characters in length ■ Must contain at least one uppercase letter ■ Must contain at least one lowercase letter ■ Must contain at least one number ■ Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!)	-	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
■ vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On ■ vCenter Server Appliance 5.5 with an external vCenter Single Sign-On ■ vCenter Server Appliance 6.0 with an embedded Platform Services Controller ■ vCenter Server Appliance 6.0 with an external Platform Services Controller	Deployment size of the new vCenter Server Appliance for your vSphere environment ■ Tiny Deploys an appliance with 2 CPUs and 10 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines. ■ Small Deploys an appliance with 4 CPUs and 16 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines. ■ Medium Deploys an appliance with 8 CPUs and 24 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines. ■ Large Deploys an appliance with 16 CPUs and 32 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines. ■ X-Large Deploys an appliance with 24 CPUs and 48 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines.	Tiny	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
■ vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On ■ vCenter Server Appliance 5.5 with an external vCenter Single Sign-On ■ vCenter Server Appliance 6.0 with an embedded Platform Services Controller ■ vCenter Server Appliance 6.0 with an external Platform Services Controller	Storage size of the new vCenter Server Appliance for your vSphere environment **Note** Consider the database size of the appliance that you want to upgrade and the types of the data that you want transfer to the new appliance. For an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance. ■ Default For tiny deployment size, deploys the appliance with 250 GB of storage. For small deployment size, deploys the appliance with 290 GB of storage. For medium deployment size, deploys the appliance with 425 GB of storage. For large deployment size, deploys the appliance with 640 GB of storage. For x-large deployment size, deploys the appliance with 980 GB of storage. ■ Large For tiny deployment size, deploys the appliance with 775 GB of storage. For small deployment size, deploys the appliance with 820 GB of storage. For medium deployment size, deploys the appliance with 925 GB of storage. For large deployment size, deploys the appliance with 990 GB of storage. For x-large deployment size, deploys the appliance with 1030 GB of storage. ■ X-Large For tiny deployment size, deploys the appliance with 1650 GB of storage. For small deployment size, deploys the appliance with 1700 GB of storage. For medium deployment size, deploys the appliance with 1805 GB of storage. For large deployment size, deploys the appliance with 1870 GB of storage. For x-large deployment size, deploys the appliance with 1910 GB of storage.	Default	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
All deployment types	Name of the datastore on which you want to store the configuration files and virtual disks of the new appliance **Note** The installer displays a list of datastores that are accessible from your target server.	-	
	Enable or disable Thin Disk Mode	Disabled	
All deployment types	Name of the network to which to connect the new appliance **Note** The installer displays a drop-down menu with networks that depend on the network settings of your target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu. The network must be accessible from the source server on which resides that appliance that you want to upgrade. The network must be accessible from the client machine from which you perform the deployment.	-	
	IP version for the appliance temporary address Can be either IPv4 or IPv6.	IPv4	
	IP assignment for the appliance temporary address Can be either static or DHCP.	static	
All deployment types Only if you use a static assignment for the temporary IP address	Temporary system name (FQDN or IP address) The system name is used for managing the local system. The system name must be FQDN. If a DNS server is not available, provide a static IP address.	-	
	Temporary IP address	-	
	For IPv4 version, a subnet mask as a dot decimal notation or a network prefix as an integer between 0 and 32 For IPv6 version, a network prefix as an integer between 0 and 128	-	
	Default gateway	-	

Table 2-5. Required Information During Stage 1 of the Upgrade (continued)

Required for Upgrade of	Required Information	Default	Your Entry
	DNS servers separated by commas	-	
All deployment types Only if you use DHCP with IPv4 and have a Dynamic DNS (DDNS) server available in your environment.	Temporary system name (FQDN)	-	

Table 2-6. Required Information During Stage 2 of the Upgrade

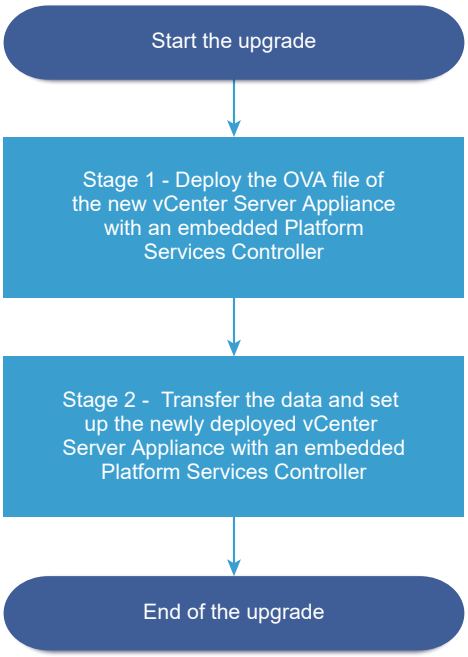
Required for	Required Information	Default	Your Entry
vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On	vCenter Single Sign-On site name	-	
■ vCenter Server Appliance 5.5 with an embedded or external vCenter Single Sign-On ■ vCenter Server Appliance 6.0 with an embedded or external Platform Services Controller	Data types to transfer from the old appliance to the new appliance In addition to the configuration data, you can transfer the events, tasks, and, performance metrics. **Note** For minimum upgrade time and storage requirement for the new appliance, select to transfer only the configuration data.	-	
■ vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On ■ vCenter Server Appliance 6.0 with an embedded Platform Services Controller ■ Platform Services Controller 6.0 appliance	Join or do not participate in the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.	Join the CEIP	

Upgrade a vCenter Server Appliance 5.5 or 6.0 with an Embedded vCenter Single Sign-On or Platform Services Controller by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance 5.5 or 6.0 that uses an embedded vCenter Single Sign-On or Platform Services Controller to vCenter Server Appliance 6.5 with an embedded Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

You can deploy version 6.5 of the vCenter Server Appliance and Platform Services Controller appliance on hosts that are running ESXi 5.5 or later and on vCenter Server instances 5.5 or later.

Figure 2-4. Upgrade Workflow of a vCenter Server Appliance with an Embedded Platform Services Controller



Prerequisites

- See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 5.5 or 6.0 or Platform Services Controller Appliance 6.0.

Procedure

1 Stage 1 - Deploy the OVA File of the New vCenter Server Appliance With an Embedded Platform Services Controller

With stage 1 of the upgrade process, you deploy the OVA file, which is included in the vCenter Server Appliance installer, for the new vCenter Server Appliance with an embedded Platform Services Controller.

2 Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance With an Embedded Platform Services Controller

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server Appliance 6.5 with an embedded Platform Services Controller.

Stage 1 - Deploy the OVA File of the New vCenter Server Appliance With an Embedded Platform Services Controller

With stage 1 of the upgrade process, you deploy the OVA file, which is included in the vCenter Server Appliance installer, for the new vCenter Server Appliance with an embedded Platform Services Controller.

Procedure

1. In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Upgrade**.
3. Review the Introduction page to understand the upgrade process and click **Next**.
4. Read and accept the license agreement, and click **Next**.

5 Connect to the source appliance that you want to upgrade.

a Enter the information about the source vCenter Server Appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade.
Appliance HTTPS port	The default value (443) is displayed and cannot be edited.

b Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important** The user must be administrator@*your_domain_name*. If you are upgrading vCenter Server Appliance 5.5.x, this is administrator@vsphere.local.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

c Enter the information about the source ESXi host or vCenter Server instance on which resides the vCenter Server Appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the source ESXi host or vCenter Server instance on which the vCenter Server Appliance that you want to upgrade resides. **Note** The source vCenter Server instance cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use the source ESXi host.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6 Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.

7 If you are upgrading from version 5.5, on the Select deployment type page, select **vCenter Server with an embedded Platform Services Controller**, and click **Next**.

8 Connect to the target server on which you want to deploy the new vCenter Server Appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance. **Note** The target server cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

9 On the Set up target appliance VM page, enter a name for the new vCenter Server Appliance, set the password for the root user, and click **Next**.

The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

Note The root password of the old appliance is not transferred to the new upgraded appliance.

10 Select the deployment size for the new vCenter Server Appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 CPUs and 10 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 16 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 24 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines

Deployment Size Option	Description
Large	Deploys an appliance with 16 CPUs and 32 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 48 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines

11 Select the storage size for the new vCenter Server Appliance, and click **Next**.

Important You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 250 GB of storage.	Deploys an appliance with 290 GB of storage.	Deploys an appliance with 425 GB of storage.	Deploys an appliance with 640 GB of storage.	Deploys an appliance with 980 GB of storage.
Large	Deploys an appliance with 775 GB of storage.	Deploys an appliance with 820 GB of storage.	Deploys an appliance with 925 GB of storage.	Deploys an appliance with 990 GB of storage.	Deploys an appliance with 1030 GB of storage.
X-Large	Deploys an appliance with 1650 GB of storage.	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1805 GB of storage.	Deploys an appliance with 1870 GB of storage.	Deploys an appliance with 1910 GB of storage.

12 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

13 Configure the temporary network for communication between the vCenter Server Appliance that you want to upgrade and the new vCenter Server Appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.

Option	Action
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

14 On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server Appliance and click **Finish** to start the OVA deployment process.

15 Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the Appliance Management Interface of the newly deployed vCenter Server Appliance to transfer the data from the old appliance and set up the services.

Results

The newly deployed vCenter Server Appliance 6.5 with an embedded Platform Services Controller is running on the target server but is not configured.

Important The data from the old appliance is not transferred and the services of the new appliance are not started.

Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance With an Embedded Platform Services Controller

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server Appliance 6.5 with an embedded Platform Services Controller.

Procedure

1 Review the introduction to stage 2 of the upgrade process and click **Next**.

2 Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.

- If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

  You cannot proceed with the upgrade until you have corrected the errors.

  Important If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.

- If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

  After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.

3 If you are upgrading version 5.5 of the vCenter Server Appliance that uses the embedded vCenter Single Sign-On instance, on the Site name configuration page, enter the site name for the vCenter Single Sign-On, and click **Next**.

  The site name must contain alphanumeric characters. Choose your own name for the vCenter Single Sign-On site. You cannot change the name after installation.

  Non-ASCII or high-ASCII characters are not supported in site names. Your site name must include alphanumeric characters and a comma (,), period (.), question mark (?), dash (-), underscore (_), plus sign (+) or equals sign (=).

4 On the Select upgrade data page, choose the types of data that you want to transfer from the old appliance to the new upgraded appliance.

  The large amount of data requires more time to be transferred to the new appliance. For minimum upgrade time and storage requirement for the new appliance, select to transfer only the configuration data.

5 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*.

6 On the ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.

7 Read the shutdown warning message and click **OK**.

8 Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

Results

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

What to do next

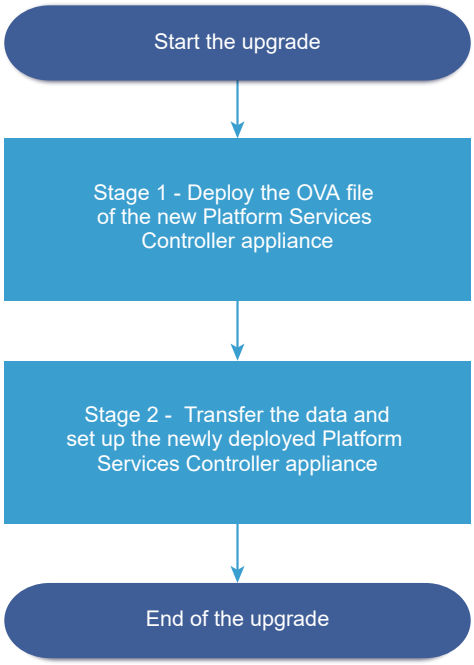
- Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.
- If the old vCenter Server Appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.
- You can configure high availability for the vCenter Server Appliance. For information about providing vCenter Server Appliance high availability, see *vSphere Availability*.

Upgrade a Platform Services Controller Appliance 6.0 by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a Platform Services Controller appliance 6.0 to version 6.5. You must run the GUI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

Important You must upgrade the replicating Platform Services Controller instances in a sequence.

Figure 2-5. Upgrade Workflow of a Platform Services Controller Appliance



Prerequisites

- See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 5.5 or 6.0 or Platform Services Controller Appliance 6.0.

Procedure

1 Stage 1 - Deploy the OVA File of the New Platform Services Controller Appliance

With stage 1 of the upgrade process, you deploy the OVA file of the new Platform Services Controller appliance 6.5.

2 Stage 2 - Transfer the Data and Set up the Newly Deployed Platform Services Controller Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed Platform Services Controller appliance 6.5.

Stage 1 - Deploy the OVA File of the New Platform Services Controller Appliance

With stage 1 of the upgrade process, you deploy the OVA file of the new Platform Services Controller appliance 6.5.

Procedure

1 In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.

- For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
- For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
- For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.

2 On the Home page, click **Upgrade**.

3 Review the Introduction page to understand the upgrade process and click **Next**.

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

5 Connect to the source appliance that you want to upgrade.

a Enter the information about the source Platform Services Controller appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance server or host name	Enter the IP address or FQDN of the Platform Services Controller appliance that you want to upgrade.
Appliance HTTPS Port	The default value (443) is displayed and cannot be edited.

b Enter the **Appliance (OS) Root password**.

c Enter the information about ESXi host or vCenter Server instance on which the Platform Services Controller appliance that you want to upgrade resides, and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the ESXi host or vCenter Server instance on which the Platform Services Controller appliance that you want to upgrade resides.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6 Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.

7 Connect to the target server on which you want to deploy the new Platform Services Controller appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

8 On the Set up target appliance VM page, enter a name for the new Platform Services Controller appliance, set the password for the root user, and click **Next**.

The name of the new Platform Services Controller appliance must be different from the name of the source appliance. The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

Note The root password of the old appliance is not transferred to the new upgraded appliance.

9 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**.

10 Configure the temporary network for communication between the Platform Services Controller appliance that you want to upgrade and the new Platform Services Controller appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

11 On the Ready to complete stage 1 page, review the deployment settings for the new Platform Services Controller appliance and click **Finish** to start the OVA deployment process.

12 Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and set up the services of the new appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the appliance management interface of the newly deployed Platform Services Controller appliance to transfer the data from the old appliance and set up the services.

Results

The newly deployed Platform Services Controller appliance 6.5 is running on the target server but is not configured.

Important The data from the old appliance is not transferred and the services of the new appliance are not started.

Stage 2 - Transfer the Data and Set up the Newly Deployed Platform Services Controller Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed Platform Services Controller appliance 6.5.

Procedure

1. Review the introduction to stage 2 of the upgrade process and click **Next**.
2. Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.
   - If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

     You cannot proceed with the upgrade until you have corrected the errors.

     Important If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.
   - If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

     After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.
3. 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*.
4. On the ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
5. Read the shutdown warning message and click **OK**.
6. Wait for the data transfer and setup process to finish and click **OK** to go to the Platform Services Controller Getting Started page.

Results

The Platform Services Controller appliance is upgraded. The old Platform Services Controller appliance is powered off and the new appliance starts.

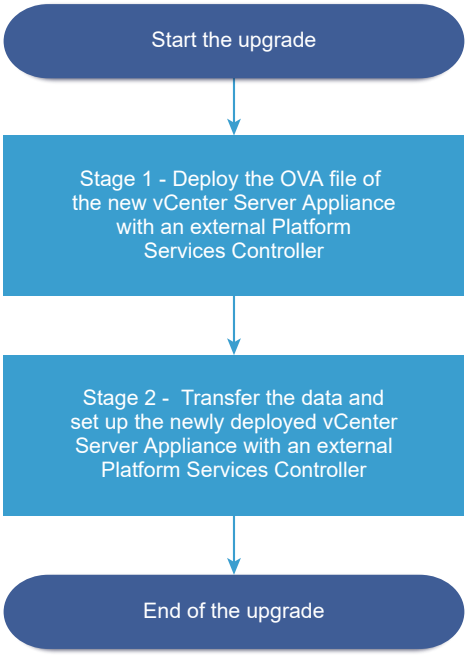
What to do next

- If the old Platform Services Controller 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*.
- If the Platform Services Controller appliance replicates the infrastructure data with other Platform Services Controller instances, you must upgrade all Platform Services Controller instances in the vCenter Single Sign-On domain to the same version.

Upgrade a vCenter Server Appliance 5.5 or 6.0 with an External vCenter Single Sign-On or Platform Services Controller Instance by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance 5.5 or 6.0 that uses an external vCenter Single Sign-On or Platform Services Controller instance to vCenter Server Appliance 6.5 with an external Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

Figure 2-6. Upgrade Workflow of a vCenter Server Appliance with an External Platform Services Controller



Prerequisites

- See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 5.5 or 6.0 or Platform Services Controller Appliance 6.0.
- Upgrade or migrate the external vCenter Single Sign-On 5.5 or Platform Services Controller 6.0 instances in the domain to Platform Services Controller 6.5.

Stage 1 - Deploy the OVA File of the New vCenter Server Appliance With an External Platform Services Controller

With stage 1 of the upgrade process, you deploy the OVA file of the new vCenter Server Appliance 6.5 with an external Platform Services Controller.

Procedure

1 In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2 On the Home page, click **Upgrade**.
3 Review the Introduction page to understand the upgrade process and click **Next**.
4 Read and accept the license agreement, and click **Next**.

5 Connect to the source appliance that you want to upgrade.

a Enter the information about the source vCenter Server Appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade.
Appliance HTTPS port	The default value (443) is displayed and cannot be edited.

b Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important** The user must be administrator@*your_domain_name*. If you are upgrading vCenter Server Appliance 5.5.x, this is administrator@vsphere.local.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

c Enter the information about the source ESXi host or vCenter Server instance on which resides the vCenter Server Appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the source ESXi host or vCenter Server instance on which the vCenter Server Appliance that you want to upgrade resides. **Note** The source vCenter Server instance cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use the source ESXi host.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6 Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.

7 If you are upgrading from version 5.5, on the Select deployment type page, select **vCenter Server with an external Platform Services Controller**, and click **Next**.

8 Connect to the target server on which you want to deploy the new vCenter Server Appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance. **Note** The target server cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

9 On the Set up target appliance VM page, enter a name for the new vCenter Server Appliance, set the password for the root user, and click **Next**.

The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

Note The root password of the old appliance is not transferred to the new upgraded appliance.

10 Select the deployment size for the new vCenter Server Appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 CPUs and 10 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 16 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 24 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines

Deployment Size Option	Description
Large	Deploys an appliance with 16 CPUs and 32 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 48 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines

11 Select the storage size for the new vCenter Server Appliance, and click **Next**.

Important You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 250 GB of storage.	Deploys an appliance with 290 GB of storage.	Deploys an appliance with 425 GB of storage.	Deploys an appliance with 640 GB of storage.	Deploys an appliance with 980 GB of storage.
Large	Deploys an appliance with 775 GB of storage.	Deploys an appliance with 820 GB of storage.	Deploys an appliance with 925 GB of storage.	Deploys an appliance with 990 GB of storage.	Deploys an appliance with 1030 GB of storage.
X-Large	Deploys an appliance with 1650 GB of storage.	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1805 GB of storage.	Deploys an appliance with 1870 GB of storage.	Deploys an appliance with 1910 GB of storage.

12 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

13 Configure the temporary network for communication between the vCenter Server Appliance that you want to upgrade and the new vCenter Server Appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.

Option	Action
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

14 On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server Appliance and click **Finish** to start the OVA deployment process.

15 Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the Appliance Management Interface of the newly deployed vCenter Server Appliance to transfer the data from the old appliance and set up the services.

Results

The newly deployed target vCenter Server Appliance 6.5 with an external Platform Services Controller is running on the target server but is not configured.

Important The data from the source vCenter Server is not transferred and the services of the target appliance are not started.

Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance With an External Platform Services Controller

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server Appliance 6.5 with an external Platform Services Controller.

Procedure

1 Review the introduction to stage 2 of the upgrade process and click **Next**.

2 Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.

- If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

  You cannot proceed with the upgrade until you have corrected the errors.

  Important If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.

- If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

  After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.

3 On the Select upgrade data page, choose the types of data that you want to transfer from the old appliance to the new upgraded appliance.

  The large amount of data requires more time to be transferred to the new appliance. For minimum upgrade time and storage requirement for the new appliance, select to transfer only the configuration data.

4 On the ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.

5 Read the shutdown warning message and click **OK**.

6 Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

Results

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

What to do next

- Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.
- 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 all vCenter Server instances in the vCenter Single Sign-On domain.
- You can configure high availability for the vCenter Server Appliance. For information about providing vCenter Server Appliance high availability, see *vSphere Availability*.

CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance

You can use the CLI installer to perform an unattended upgrade of a vCenter Server Appliance or Platform Services Controller appliance on an ESXi host or vCenter Server instance.

The CLI upgrade process includes downloading the vCenter Server Appliance installer on a network virtual machine or physical server from which you want to perform the upgrade, preparing a JSON configuration file with the upgrade information, and running the upgrade command.

Important The user name that you use to log in to the machine from which you want to run the CLI upgrade, the path to the vCenter Server Appliance ISO file, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

The vCenter Server Appliance ISO file contains templates of JSON files that contain the minimum configuration parameters that are required for upgrading a vCenter Server Appliance or Platform Services Controller appliance. For information about preparing JSON templates for CLI upgrade of the vCenter Server Appliance and Platform Services Controller appliance, see Prepare Your JSON Configuration File for CLI Upgrade.

Important For topologies with external Platform Services Controller instances, you must upgrade the replicating Platform Services Controller instances in a sequence. After the successful upgrade of all Platform Services Controller instances in the domain, you can perform concurrent upgrades of multiple vCenter Server appliances that point to a common external Platform Services Controller instance.

Prepare Your JSON Configuration File for CLI Upgrade

Before you run the CLI command to upgrade a vCenter Server Appliance or Platform Services Controller appliance, you must prepare a JSON file with configuration parameters and their values for your upgrade specification.

The vCenter Server Appliance installer contains JSON templates for all upgrade types. For information about the templates, see JSON Templates for CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance.

You can upgrade an appliance with minimum configurations by setting values to the configuration parameters in the JSON template for your specification. You can edit the preset values, remove configuration parameters, and add configuration parameters for custom configurations.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run the `vcsa-deploy upgrade --template-help` command or see Upgrade Configuration Parameters.

Prerequisites

- You must be familiar with the JSON syntax.
- Download and Mount the vCenter Server Appliance Installer.

Procedure

1. In the vCenter Server Appliance installer, navigate to the `vcsa-cli-installer` directory, and open the `templates` subfolder.
2. Copy the upgrade templates from the `upgrade` subfolder to your workspace.

   Important The path to the JSON configuration files must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

3. Open the template file for your use case in a text editor.

   To ensure the correct syntax of your JSON configuration file, use a JSON editor.

4. Fill in the values for the required configuration parameters and, optionally, enter additional parameters and their values.

   For example, if you want to use an IPv4 DHCP assignment for the temporary network of the new appliance, in the `temporary.network` subsection of the template, change the value of the `mode` parameter to `dhcp` and remove the default configuration parameters that are for a static assignment.

   ```
   "temporary.network": {
       "ip.family": "ipv4",
       "mode": "dhcp"
   },
   ```

   Important The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

   To set a value that contains a backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-6.5.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-6.5.0.XXXX-YYYYYYY_OVF10.ova`.

   The Boolean values must contain only lowercase characters, that is, a value can be either `true` or `false`. For example, `"ssh.enable":false`.

5. (Optional) Use a JSON editor of your choice to validate the JSON file.
6. Save in UTF-8 format and close the file.

What to do next

You can create and save additional templates if needed for your upgrade specification.

JSON Templates for CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance

The vCenter Server Appliance installer contains JSON templates that are located in the `vcsa-cli-installer/templates` directory. In the `upgrade` subfolder, you can find the JSON templates with the minimum configuration parameters for all upgrade types.

For each upgrade type, there is one template for deploying the new appliance on an ESXi host and another template for deploying the new appliance on a vCenter Server instance.

Table 2-7. Upgrade JSON Templates Included in the vCenter Server Appliance Installer

Location	Template	Description
`vcsa-cli-installer\templates\upgrade\vcsa5.5`	`embedded_vCSA_on_ESXi.json`	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On to vCenter Server Appliance 6.5 with an embedded Platform Services Controller on an ESXi host.
	`embedded_vCSA_on_VC.json`	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On to vCenter Server Appliance 6.5 with an embedded Platform Services Controller on a vCenter Server instance.
	`vCSA_on_ESXi.json`	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 5.5 with an external vCenter Single Sign-On to vCenter Server Appliance 6.5 with an external Platform Services Controller on an ESXi host.
	`vCSA_on_VC.json`	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 5.5 with an external vCenter Single Sign-On to vCenter Server Appliance 6.5 with an external Platform Services Controller on a vCenter Server instance.

Table 2-7. Upgrade JSON Templates Included in the vCenter Server Appliance Installer (continued)

Location	Template	Description
vcsa-cli-installer\templates\upgrade\vcsa6.0	embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.0 with an embedded Platform Services Controller to vCenter Server Appliance 6.5 with an embedded Platform Services Controller on an ESXi host.
	embedded_vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.0 with an embedded Platform Services Controller to vCenter Server Appliance 6.5 with an embedded Platform Services Controller on a vCenter Server instance.
	PSC_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a Platform Services Controller appliance 6.0 to Platform Services Controller appliance 6.5 on an ESXi host.
	PSC_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a Platform Services Controller appliance 6.0 to Platform Services Controller appliance 6.5 on a vCenter Server instance.
	vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.0 with an external Platform Services Controller to vCenter Server Appliance 6.5 with an external Platform Services Controller on an ESXi host.
	vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.0 with an external Platform Services Controller to vCenter Server Appliance 6.5 with an external Platform Services Controller on a vCenter Server instance.

Upgrade Configuration Parameters

When you prepare your JSON configuration files for CLI upgrade, you must set parameters and values to provide input data for the upgrade of a vCenter Server Appliance or Platform Services Controller appliance.

Sections and Subsections of Configuration Parameters in the JSON Upgrade Files

The configuration parameters in the JSON configuration files for CLI upgrade are organized in sections and subsections.

Table 2-8. Sections and Subsections of Configuration Parameters in the JSON Upgrade Files

Section	Subsection	Description
`new.vcsa` - describes the new appliance that you want to deploy	`esxi`	Use only if you want to deploy the new appliance directly on an ESXi host. Contains the configuration parameters that describe the target ESXi host. See Table 2-9. Configuration Parameters in the new.vcsa Section, esxi Subsection. **Note** You must fill in either this subsection or the `vc` subsection.
	`vc`	Use only if you want to deploy the new appliance on the inventory of a vCenter Server instance. Contains the configuration parameters that describe the target ESXi host or DRS cluster from the vCenter Server inventory. See Table 2-10. Configuration Parameters in the new.vcsa Section, vc Subsection. **Note** You must fill in either this subsection or the `esxi` subsection. The target vCenter Server instance cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use the `esxi` subsection.
	`appliance`	Contains the configuration parameters that describe the new appliance. See Table 2-11. Configuration Parameters in the new.vcsa Section, appliance Subsection
	`os`	Contains only the `ssh.enable` configuration parameter to set the SSH administrator login to the new appliance. See Table 2-12. Configuration Parameters in the new.vcsa Section, os Subsection
	`ovftool.arguments`	Optional. Use this subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates. **Important** The vCenter Server Appliance installer does not validate the configuration parameters in the `ovftool.arguments` subsection. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
	`sso`	Contains only the `site-name` configuration parameter to set a vCenter Single Sign-On site for the new appliance. See Table 2-13. Configuration Parameters in the new.vcsa Section, sso Subsection. Required only if you are upgrading a vCenter Server Appliance 5.5 with an embedded Platform Services Controller.
	`temporary.network`	Contains the configuration parameters that describe the temporary network settings for the new appliance. See Table 2-14. Configuration Parameters in the new.vcsa Section, temporary.network Subsection

Table 2-8. Sections and Subsections of Configuration Parameters in the JSON Upgrade Files (continued)

Section	Subsection	Description
	`user-options`	Contains only the `vcdb.migrateSet` configuration parameter to set the types of data that you want to transfer from the old appliance to the new appliance. See Table 2-15. Configuration Parameters in the new.vcsa Section, user-options Subsection
`source.vc` - describes the existing appliance that you want to upgrade	`esxi`	Contains the configuration parameters that describe the source ESXi host on which resides the appliance that you want to upgrade. See Table 2-16. Configuration Parameters in the source.vc Section, esxi Subsection.
	`vc.vcsa`	Contains the configuration parameters that describe the source appliance that you want to upgrade. See Table 2-17. Configuration Parameters in the source.vc Section, vc.vcsa Subsection.
`source.vum` - describes the source VMware Update Manager instance Use if you want to automatically run the Migration Assistant on the VMware Update Manager instance.	`run.migration.assistant`	Optional if the source vCenter Server Appliance that you want to upgrade is connected to a VMware Update Manager instance that runs on a Windows virtual machine. Use this subsection if you want to automatically run the Migration Assistant on the source VMware Update Manager instance. Contains the configuration parameters that describe the source VMware Update Manager instance, which will be migrated to the new upgraded vCenter Server Appliance. See Table 2-18. Configuration Parameters in the source.vum Section, run.migration.assistant Subsection. **Note** The Migration Assistant uses port 9123 by default. If port 9123 is used by another service on the your Update Manager machine, the Migration Assistant automatically finds another free port. You cannot set a custom port for the Migration Assistant.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP)	`settings`	Contains only the `ceip.enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). See Table 2-19. Configuration Parameters in the ceip Section, settings Subsection. Required only if you are upgrading a vCenter Server Appliance with an embedded Platform Services Controller, vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On, or a Platform Services Controller appliance. **Note** If the `ceip.enabled` configuration parameter is set to `true`, you must run the CLI deployment command with the `--acknowledge-ceip` argument. For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

Important The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains a backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-6.5.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-6.5.0.XXXX-YYYYYYY_OVF10.ova`.

The Boolean values must contain only lowercase characters. Can be either `true` or `false`. For example, `"ssh.enable":false`.

Configuration Parameters in the `new.vcsa` Section

Table 2-9. Configuration Parameters in the `new.vcsa` Section, `esxi` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target ESXi host on which you want deploy the new appliance.
`username`	string	A user name with administrative privileges on the target ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the target ESXi host.
`deployment.network`	string	The name of the network to which to connect the new appliance. The network must part of the target ESXi host network configuration. **Note** The network must be accessible from the source ESXi host on which resides the appliance that you want to upgrade. The network must be also accessible from the client machine from which you are performing the upgrade. Ignored if the target ESXi host has only one network.
`datastore`	string	The name of the datastore on which to store the virtual machine configuration files and virtual disks of the new appliance. The datastore must be available to the target ESXi host. **Note** The datastore must have at least 25 GB of free space.
`port`	integer	The HTTPS reverse proxy port of the target ESXi host. The default port is 443. Use only if the target ESXi host uses a custom HTTPS reverse proxy port.

Table 2-10. Configuration Parameters in the `new.vcsa` Section, `vc` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target vCenter Server instance on which you want deploy the new appliance.
`username`	string	vCenter Single Sign-On administrator user name on the target vCenter Server instance, for example, administrator@vsphere.local.
`password`	string	The password of the vCenter Single Sign-On administrator user on the target vCenter Server instance.

Table 2-10. Configuration Parameters in the `new.vcsa` Section, `vc` Subsection (continued)

Name	Type	Description
`deployment.network`	string	The name of the network to which to connect the new appliance. The network must part of the target ESXi host or DRS cluster network configuration. **Note** The network must be accessible from the source ESXi host on which resides the appliance that you want to upgrade. The network must be also accessible from the client machine from which you are performing the upgrade. Ignored if the target ESXi host or DRS cluster has only one network.

`datacenter`	string or array	The vCenter Server datacenter that contains the target ESXi host or DRS cluster on which you want to deploy the new appliance.
		If the datacenter is located in a folder or a structure of folders, the value must be either a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "datacenter_name"]`
		or
		`"parent_folder, child_folder, datacenter_name"`
		Note The value is case-sensitive.

`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the new appliance. **Note** The datastore must be available to the target ESXi host or DRS cluster. The datastore must have at least 25 GB of free space.
`port`	integer	The HTTPS reverse proxy port of the target vCenter Server instance. The default port is 443. Use only if the target vCenter Server instance uses a custom HTTPS reverse proxy port.

Table 2-10. Configuration Parameters in the `new.vcsa` Section, `vc` Subsection (continued)

Name	Type	Description

`target`	string or array	The target ESXi host or DRS cluster on which you want to deploy the new appliance.
		
		Important You must provide the name that is displayed in the vCenter Server inventory. For example, if the name of the target ESXi host is an IP address in the vCenter Server inventory, you cannot provide an FQDN.
		
		If the target ESXi host or DRS cluster is located in a folder or a structure of folders, the value must be a comma-separated list of strings or a comma-separated list as a single string. For example,
		
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		
		or
		
		`"parent_folder, child_folder, esxi-host.domain.com"`
		
		If the target ESXi host is part of a cluster, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		
		`["cluster_name", "esxi-host.domain.com"]`
		
		or
		
		`"cluster_name, esxi-host.domain.com"`
		
		Note The value is case-sensitive.

`vm.folder`	string	Optional. The name of the VM folder to which to add the new appliance.

Table 2-11. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection

Name	Type	Description
`thin.disk.mode`	Boolean	Set to `true` to deploy the new appliance with thin virtual disks.
`deployment.option`	string	The size for the new appliance. **Note** You must consider the database size of the appliance that you want to upgrade. For an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance. ■ Set to `tiny` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 250 GB of storage. ■ Set to `tiny-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 775 GB of storage. ■ Set to `tiny-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 1650 GB of storage. ■ Set to `small` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 290 GB of storage. ■ Set to `small-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 820 GB of storage. ■ Set to `small-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1700 GB of storage. ■ Set to `medium` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 425 GB of storage. ■ Set to `medium-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the large storage size.

Table 2-11. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 8 CPUs, 24 GB of memory, and 925 GB of storage. ■ Set to `medium-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1805 GB of storage. ■ Set to `large` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 640 GB of storage. ■ Set to `large-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 990 GB of storage. ■ Set to `large-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1870 GB of storage. ■ Set to `xlarge` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 980 GB of storage. ■ Set to `xlarge-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1030 GB of storage. ■ Set to `xlarge-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1910 GB of storage. ■ Set to `management-tiny` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 250 GB of storage. ■ Set to `management-tiny-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the large storage size.

Table 2-11. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 2 CPUs, 10 GB of memory, and 775 GB of storage. ■ Set to `management-tiny-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 1650 GB of storage. ■ Set to `management-small` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 290 GB of storage. ■ Set to `management-small-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 820 GB of storage. ■ Set to `management-small-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1700 GB of storage. ■ Set to `management-medium` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 425 GB of storage. ■ Set to `management-medium-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 925 GB of storage. ■ Set to `management-medium-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1805 GB of storage. ■ Set to `management-large` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 640 GB of storage. ■ Set to `management-large-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the large storage size.

Table 2-11. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 16 CPUs, 32 GB of memory, and 990 GB of storage. ■ Set to `management-large-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1870 GB of storage. ■ Set to `management-xlarge` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 980 GB of storage. ■ Set to `management-xlarge-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1030 GB of storage. ■ Set to `management-xlarge-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1910 GB of storage. ■ Set to `infrastructure`if you want to deploy a Platform Services Controller appliance. Deploys an appliance with 2 CPUs, 4 GB of memory, and 60 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server Appliance installation package. By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the new appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool.path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 2-12. Configuration Parameters in the `new.vcsa` Section, `os` Subsection

Name	Type	Description
`ssh.enable`	Boolean	Set to `true` to enable SSH administrator login to the new appliance.

Table 2-13. Configuration Parameters in the `new.vcsa` Section, `sso` Subsection

Name	Type	Description
`site-name`	string	vCenter Single Sign-On site name for the new appliance. Required only if you are upgrading a vCenter Server Appliance 5.5 with an embedded vCenter Single Sign-On

Table 2-14. Configuration Parameters in the `new.vcsa` Section, `temporary.network` Subsection

Name	Type	Description
`ip.family`	string	IP version for the temporary network of the new appliance. Set to `ipv4` or `ipv6`.
`mode`	string	IP assignment for the temporary network of the new appliance. Set to `static` or `dhcp`.
`ip`	string	Temporary IP address for the new appliance. Required only if you use static assignment, that is, if you set the `mode` parameter to `static`. You must set an IPv4 or IPv6 address that corresponds to the temporary network IP version, that is, to the value of the `ip.family` parameter. An IPv4 address must comply with the RFC 790 guidelines. An IPv6 address must comply with the RFC 2373 guidelines.

`dns.servers`	string or array	IP addresses of one or more DNS servers for the temporary network of the new appliance.
		To set more than one DNS server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`
		Required only if you use static network mode for the temporary IP address allocation, that is, if you set the `mode` parameter to `static`.

`prefix`	string	Network prefix length for the temporary network of the new appliance. Use only if the `mode` parameter is set to `static`. Remove if the `mode` parameter is set to `dhcp`. The network prefix length is the number of bits that are set in the subnet mask. For example, if the subnet mask is 255.255.255.0, there are 24 bits in the binary version of the prefix length, so the network prefix length is 24. For IPv4 version, the value must be between `0` and `32`. For IPv6 version, the value must be between `0` and `128`.

Table 2-14. Configuration Parameters in the `new.vcsa` Section, `temporary.network` Subsection (continued)

Name	Type	Description
`gateway`	string	IP address of the default gateway for the temporary network of the new appliance. For IPv6 version, the value can be `default`.
`system.name`	string	Primary network identity for the temporary network of th new appliance. Can be an IP address or FQDN, preferably FQDN. The FQDN and dotted-decimal numbers must comply with the RFC 1123 guidelines.

Table 2-15. Configuration Parameters in the `new.vcsa` Section, `user-options` Subsection

Name	Type	Description
`vcdb.migrateSet`	string	The types of data to transfer from the old appliance to the new appliance. ■ Set to `core` if you want to transfer only the configuration data. ■ Set to `all` if you want to transfer the configuration, events, tasks, and performance metrics data. ■ Set to `core_events_tasks` if you want to transfer the configuration, events, and tasks data. **Note** For minimum upgrade time and storage requirement for the new appliance, use the `core` value.

Configuration Parameters in the `source.vc` Section

Table 2-16. Configuration Parameters in the `source.vc` Section, `esxi` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the source ESXi host on which resides the appliance that you want to upgrade.
`username`	string	A user name with administrative privileges on the source ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the source ESXi host.
`port`	integer	The HTTPS reverse proxy port of the source ESXi host. The default port is 443. Use only if the source ESXi host uses a custom HTTPS reverse proxy port.

Table 2-17. Configuration Parameters in the `source.vc` Section, `vc.vcsa` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the source appliance that you want to upgrade.
`username`	string	vCenter Single Sign-On administrator user on the source appliance, for example administrator@vsphere.local. **Important** The user must be administrator@*your_domain_name*.

Table 2-17. Configuration Parameters in the `source.vc` Section, `vc.vcsa` Subsection (continued)

Name	Type	Description
`password`	string	The password of the vCenter Single Sign-On administrator user on the source appliance.
`root.password`	string	The password for the root user of the operating system of the source appliance.

Configuration Parameters in the `source.vum` Section

Table 2-18. Configuration Parameters in the `source.vum` Section, `run.migration.assistant` Subsection

Name	Type	Description
`esxi.hostname`	string	The IP address or FQDN of the ESXi host on which resides the source VMware Update Manager instance. If an FQDN is provided, it must be resolvable from the client machine from which you run the upgrade.
`esxi.username`	string	A user name with administrative privileges on the ESXi host, for example, root.
`esxi.password`	string	The password of the user with administrative privileges on the ESXi host.
`esxi.port`	string	The HTTPS reverse proxy port of the ESXi host. The default port is 443. Use only if the ESXi host uses a custom HTTPS reverse proxy port.
`vum.hostname`	string	The IP address or FQDN of the Windows virtual machine on which the source VMware Update Manager instance runs. If an FQDN is provided, it must be resolvable from the client machine from which you run the upgrade.
`vum.os.username`	string	The administrator user name of the Windows virtual machine on which the source VMware Update Manager instance runs.
`vum.os.password`	string	The administrator password of the Windows virtual machine on which the source VMware Update Manager instance runs. If not provided, you are prompted to enter the password at the command console during the template verification.
`export.dir`	string	Directory to export source configuration and data.

Configuration Parameters in the `ceip` Section

Table 2-19. Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
`ceip.enabled`	Boolean	Set to `true` to join the CEIP for the new upgraded appliance.

Upgrade a vCenter Server Appliance or Platform Services Controller Appliance by Using the CLI

You can use the CLI installer to perform an unattended upgrade of a vCenter Server Appliance or Platform Services Controller appliance. You must run the CLI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

Prerequisites

- See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- Prepare Your JSON Configuration File for CLI Upgrade.
- Review the arguments for running the CLI upgrade. See Syntax of the CLI Upgrade Command.
- Verify that the user name with which you are logged in to your machine, the path to the vCenter Server Appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Procedure

1. Navigate to the `vcsa-cli-installer` subdirectory for your operating system.
   - If you are running the upgrade on Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are running the upgrade on Windows OS Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are running the upgrade on Windows OS Mac OS, navigate to the `vcsa-cli-installer/mac` directory.
2. (Optional) Run a basic template verification to verify that you prepared the upgrade template correctly.

   ```
   vcsa-deploy upgrade --verify-template-only path_to_the_json_file
   ```

3. (Optional) Run a pre-upgrade check to gather and validate the upgrade requirements.

   ```
   vcsa-deploy upgrade --precheck-only path_to_the_json_file
   ```

   The pre-upgrade check installs the Upgrade Runner on the source appliance that you want to upgrade without upgrading the appliance.

   The Upgrade Runner validates the configurations such as ESXi, network settings, and NTP servers. The Upgrade Runner also checks if you have selected a suitable deployment size and storage size for the new appliance against the compute resources required for the upgrade.

4 Perform the upgrade by running the following command.

```
vcsa-deploy upgrade --accept-eula --acknowledge-ceip optional_arguments
path_to_the_json_file
```

Use *optional_arguments* to enter space-separated arguments to set additional execution parameters of the upgrade command.

For example, you can set the location of the log and other output files that the installer generates.

```
vcsa-deploy upgrade --accept-eula --acknowledge-ceip --log-dir=path_to_the_location
path_to_the_json_file
```

What to do next

Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

Syntax of the CLI Upgrade Command

You can use command arguments to set the execution parameters of the upgrade command.

You can add a space-separated list of arguments to the CLI upgrade command.

```
vcsa-deploy upgrade path_to_the_json_file list_of_arguments
```

Argument	Description
`--accept-eula`	Accepts the end-user license agreement. Required for executing the deployment command.
`--acknowledge-ceip`	Confirms your acknowledgement of your VMware Customer Experience Improvement Program (CEIP) participation. Required if the `ceip.enabled` parameter is set to `true` in the JSON deployment template.
`-v`, `--verbose`	Adds debug information to the console output.
`-t`, `--terse`	Hides the console output. Displays only warning and error messages.
`--log-dir` *LOG_DIR*	Sets the location of the log and other output files.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters in the JSON file and deploys the appliance. Does not perform verification of the OVF Tool parameters.
`--no-esx-ssl-verify`	Skips the SSL verification for ESXi connections. **Important** Avoid using this option because it might cause problems during upgrade or after upgrade because of not validated identity of the target host.

Argument	Description
`--deployment-target-ssl-thumbprint` *TARGET_THUMBPRINT*	Thumbprint to pass to the OVF Tool for verifying the target ESXi host or vCenter Server instance on which you want to deploy the new appliance.
`--pause-on-warnings`	Pauses and waits for acknowledgment of warnings.
`--verify-template-only`	Performs only the basic template verification. Does not run additional prechecks and does not deploy the new appliance.
`--precheck-only`	Installs Upgrade Runner on the source appliance and runs a complete set of prechecks without performing the upgrade.
`-h`, `--help`	Displays the help message for the `vcsa-deploy upgrade` command.
`--template-help`	Displays the help message for the use of configuration parameters in the JSON upgrade file.

After the execution finishes, you can get the exit code of the command.

Exit Code	Description
0	Command ran successfully
1	Runtime error
2	Validation error
3	Template error

Upgrading vCenter Server for Windows

3

You can upgrade vCenter Server version 5.5 and version 6.0 deployments for Windows to vCenter Server version 6.5 deployments for Windows.

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

This chapter includes the following topics:

About the vCenter Server for Windows Upgrade Process

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

You can upgrade the following deployments:

Table 3-1. Supported vSphere Upgrade Paths

Before Upgrade	After Upgrade
vCenter Server 5.5 with an embedded vCenter Single Sign-On on Windows	vCenter Server 6.5 with an embedded Platform Services Controller on Windows
vCenter Server 6.0 with an embedded Platform Services Controller instance on Windows	
vCenter Single Sign-On 5.5 on Windows	Platform Services Controller 6.5 on Windows
Platform Services Controller 6.0 on Windows	
vCenter Server 5.5 on Windows	vCenter Server 6.5 on Windows
vCenter Server 6.0 on Windows	

For upgrade steps for a vCenter Server 5.5 deployment, see Upgrading vCenter Server 5.5 on Windows . For upgrade steps for a vCenter Server 5.5 deployment, see Upgrading vCenter Server 6.0 on Windows .

Important You cannot change your deployment type during upgrade.

You cannot uninstall or reinstall individual services during the upgrade process. For example, vSphere Auto Deploy can no longer be deployed separately as it was in vCenter Server 5.5. It is part of the vCenter Server group of services for vCenter Server 6.5. For details on upgrading from 5.5 with distributed services, see Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration.

Note Starting with vSphere 6.5, the vCenter Server services are not standalone services under Windows SCM, instead they run as child processes of the VMware Service Lifecycle Manager service.

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 services. See Synchronizing Clocks on the vSphere Network.
- Verify that the system network name of the machines running vCenter Server services are valid, and are reachable from other machines in the network.
- Verify that the host name of the virtual machine or physical server on which you are installing or upgrading vCenter Server 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)**

  Note Starting with vSphere 6.5, the vCenter Server services run as child processes of the VMware Service Lifecycle Manager service.

- Verify that the local policy of the virtual machine or physical server on which you are installing or upgrading vCenter Server allows assigning **Log on as a batch job** rights to new local users.

  Note Starting with vSphere 6.5, some vCenter Server processes use separate local users that are automatically created and added to the local security policy **Log on as a batch job**. Such new local users are cm, content-library, eam, imagebuilder, mbcs, netdumper, perfcharts, rbd, vapiEndpoint, vmware-vpostgres, vsan-health, vsm, vsphere-client, and vsphere-ui.

- 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.

Pre-Install Checks for vCenter Server and Platform Services Controller on Windows

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

When you upgrade vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) vCenter Single Sign-On is included as part of the Platform Services Controller. During the upgrade of an external Platform Services Controller, the installer provides you with the option to upgrade the existing vCenter Single Sign-On server domain. During the upgrade of vCenter Server with an external Platform Services Controller, the installer prompts you to join an existing vCenter Single Sign-On server domain. When you provide the information about the 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

For information about the minimum storage requirements, see Storage Requirements for vCenter Server and Platform Services Controller on Windows . For information about the minimum hardware requirements, see Hardware Requirements for vCenter Server and Platform Services Controller on Windows .

Hardware Requirements for vCenter Server and Platform Services Controller on Windows

When you upgrade vCenter Server or Platform Services Controller 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 3-2. 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)	vCenter Server with an Embedded or External Platform Services Controller for X-Large Environment (up to 2,000 Hosts, 35,000 Virtual Machines)
Number of CPUs	2	2	4	8	16	24
Memory	4 GB RAM	10 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM	48 GB RAM

Note If you want to add an ESXi host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, your vCenter Server instance must be suitable for a large or x-large environment.

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

Storage Requirements for vCenter Server and Platform Services Controller on Windows

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

The storage requirements per folder depend on the vCenter Server services deployed on the machine, the upgrade deployment model, and the size of your vSphere 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 services and the vSphere inventory size.

Table 3-3. 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

Software Requirements for vCenter Server and Platform Services Controller on Windows

Verify 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.

Prior to upgrading or migrating vCenter Server, you must install the Microsoft Update for Universal C Runtime in Windows. See Update for Universal C Runtime in Windows.

Database Requirements for vCenter Server on Windows

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.

For information about supported database server versions, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

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.

vCenter Server is accessed through 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. For the list of all supported ports and protocols in vCenter Server, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/.

During installation, if a port is in use or is blocked using a denylist, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation.

VMware uses designated ports for communication. Also, the managed hosts monitor designated ports for data from vCenter Server. If a built-in 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.

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.

DNS Requirements for vCenter Server and Platform Services Controller on Windows

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.

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 plan to use an FQDN for the virtual machine or physical server, you must verify that the FQDN is resolvable.

You can use the `nslookup` command to verify that the DNS reverse lookup service returns an FQDN when queried with the IP address and to verify that the FQDN is resolvable.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

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 6.5 requires Adobe Flash Player v. 16 to 23. For best performance and security fixes, use Adobe Flash Player 23.

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 3-4. Supported Guest Operating Systems and Minimum Browser Versions for the vSphere Web Client

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Edge v. 79 to 86. Mozilla Firefox v. 60 to 84. Google Chrome v. 75 to 86.
Mac OS	Microsoft Edge v. 79 to 86. Mozilla Firefox v. 60 to 84. Google Chrome v. 75 to 86.

Before Upgrading vCenter Server

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

- Verify Basic Compatibility Before Upgrading vCenter Server

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

- Download the vCenter Server Installer for Windows

  Download the `.iso` installer for vCenter Server for Windows and the associated vCenter Server components and support tools.

- Preparing a vCenter Server Database for Upgrade

  vCenter Server requires a database to store and organize server data. You can either upgrade your embedded database to the bundled PostgreSQL database, or you can continue to use your external database.

- Preparing for Upgrading the Content Library

  When upgrading from vCenter Server version 6.0 or earlier, you must prepare your environment before upgrading the Content Library to prevent pre-check errors.

- Verify Network Prerequisites Before Upgrading

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

- Verify Load Balancer Before Upgrading vCenter Server

  If you are using a load balancer for high availability for vCenter Single Sign-On or Platform Services Controller, you must verify that it is supported and configured correctly before upgrading to vCenter Server 6.5.

- Prepare ESXi Hosts for vCenter Server Upgrade

  Before upgrading to vCenter Server 6.5, you must prepare your ESXi hosts.

- Verify Preparations Are Complete for Upgrading vCenter Server

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

Verify Basic Compatibility Before Upgrading vCenter Server

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

Prerequisites

Verify that your system meets the hardware and software requirements. See vCenter Server for Windows Requirements and System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance

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 must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

   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 ESXi 5.0 or ESXi 5.1 hosts to version 5.5.

4 If you have ESXi 5.0 or ESXi 5.1 hosts that you choose not to upgrade, you must remove them from the vCenter Server inventory.

Download the vCenter Server Installer for Windows

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 Log in to VMware Customer Connect.

2 Navigate to **Products and Accounts > All Products**.

3 Find VMware vSphere and click **View Download Components**.

4 Select a VMware vSphere version from the **Select Version** drop-down.

5 Select a version of VMware vCenter Server and click **GO TO DOWNLOADS**.

6 Download the vCenter Server for Windows ISO image.

7 Confirm that the md5sum is correct by using an MD5 checksum tool.

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

Preparing a vCenter Server Database for Upgrade

vCenter Server requires a database to store and organize server data. You can either upgrade your embedded database to the bundled PostgreSQL database, or you can continue to use your external database.

vCenter Server for Windows supports Oracle and Microsoft SQL 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.

For information about setting up and configuring a database, see *vSphere Installation and Setup*.

The database passwords are stored in clear text on the Windows virtual machine or physical host on which you upgrade vCenter Server and in the vCenter Server Appliance. The files containing the passwords are protected by using the operating system protection, that is, you must be a Windows local administrator or a Linux root user to access and read these files.

vCenter Server instances cannot share the same database schema. Multiple vCenter Server databases can reside on the same database server, or they can be separated across multiple database servers. For Oracle databases, which have the concept of schema objects, you can run multiple vCenter Server instances in a single database server if you have a different schema owner for each vCenter Server instance. You can also use a dedicated Oracle database server for each vCenter Server instance.

You cannot upgrade vCenter Server and point to an older external vCenter Server database. You can upgrade the vCenter Server 5.5 or 6.0 database to the latest version only by upgrading the vCenter Server instance connected to that database.

Prepare an Oracle Database for Upgrading vCenter Server

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 Database Requirements for vCenter Server on Windows .

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 5.5 to vCenter Server 6.5.

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 For vCenter Server 5.5, run the cleanup script.

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

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

c Run the cleanup script.

`@path`cleanup_orphaned_data_Oracle.sql

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

11 Make a full backup of the vCenter Server 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 vCenter Server

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 not supported for vCenter Server 6.5. The vCenter Server 5.5 embedded Microsoft SQL Server Express database is replaced with an embedded PostgreSQL database during the upgrade to vCenter Server 6.5. 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 Database Requirements for vCenter Server on Windows .

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 5.5 to vCenter Server 6.5.

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 For vCenter Server 5.5, run the cleanup script.

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

b Log in to your database.

- For Microsoft SQL Server Express, open a command prompt.
- For Microsoft SQL Server, log in to a Microsoft SQL Server Management Studio session as the vCenter Server database user.

c Run the cleanup script.

For Microsoft SQL Server Express, run: **`sqlcmd -E -S localhost\VIM_SQLEXP -d VIM_VCDB -i pathcleanup_orphaned_data_MSSQL.sql`**

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.

11 Make a full backup of the vCenter Server 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 vCenter Server

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/vpostgres/9.4/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.

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 3-5. 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	

Table 3-5. Microsoft SQL Database Permissions for vCenter Server (continued)

Permission	Description
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Necessary for running a stored procedure in the db schema.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Necessary for deploying SQL Server jobs. These permissions are mandatory only during installation and upgrade and not required after deployment.
GRANT SELECT ON msdb.dbo.sysjobsteps TOVC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
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 3-6. Oracle Database Permissions for vCenter Server

Permission	Description
GRANT CONNECT TO VPXADMIN	Necessary for connecting to the Oracle database.
GRANT RESOURCE TO VPXADMIN	Necessary for creating a trigger, sequence, type, procedure, and so on. By default, the RESOURCE role has the CREATE PROCEDURE, CREATE TABLE, and CREATE SEQUENCE privileges assigned. If the RESOURCE role lacks these privileges, grant them to the vCenter Server database user.

Table 3-6. Oracle Database Permissions for vCenter Server (continued)

Permission	Description
GRANT CREATE VIEW TO VPXADMIN	Necessary for creating a view.
GRANT CREATE SEQUENCE TO VPXADMIN	Necessary for creating a sequence.
GRANT CREATE TABLE TO VPXADMIN	Necessary for creating a table.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Necessary for creating a materialized view.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Necessary for guaranteeing that the vCenter Server database is used by a single vCenter Server instance.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Necessary during installation or upgrade for scheduling and managing the SQL jobs. This permission is not required after deployment.
GRANT SELECT ON dba_lock TO VPXADMIN	Necessary for determining existing locks on the vCenter Server database.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Necessary during upgrade for determining the required disk space. This permission is not required after deployment.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Necessary during upgrade for determining the required disk space. This permission is not required after deployment.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necessary for monitoring the free space while vCenter Server is working.
GRANT SELECT ON v_$session TO VPXADMIN	View used to determine existing locks on the vCenter Server database.
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Necessary for granting unlimited tablespace permissions to the vCenter Server database user.
GRANT SELECT ON v_$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 on the same machine on which vCenter Server is to be installed, and you changed the machine name, 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. To test this condition, ping 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.

Results

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

Preparing for Upgrading the Content Library

When upgrading from vCenter Server version 6.0 or earlier, you must prepare your environment before upgrading the Content Library to prevent pre-check errors.

If you are upgrading from vCenter Server version 6.0 or 5.5, your environment must meet upgrade requirements for the Content Library:

- All ESXi hosts from the source vCenter Server inventory must be supported by the destination vCenter Server 6.5.
- The source vCenter ServerContent Libraries must be backed by either Remote File System or Datastores. You cannot use libraries backed by local file system of the vCenter Server.
- All the remote file system shares used as library backings must be accessible at the time of the upgrade.
- No subscribed libraries are using file based subscription URI.

If you are upgrading from vCenter Server 6.0 Update 1, no actions are necessary.

If your environment does not meet the requirements, you must perform the following actions to prepare for upgrade.

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 or Platform Services Controller, you must verify that it is supported and configured correctly before upgrading to vCenter Server 6.5.

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 http://kb.vmware.com/kb/2112736 for vCenter Single Sign-On 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 Deployment Guide*.

Prepare ESXi Hosts for vCenter Server Upgrade

Before upgrading to vCenter Server 6.5, you must prepare your ESXi hosts.

Prerequisites

To upgrade vCenter Server, your ESXi hosts must be at version 5.5. If your ESXi hosts are at an earlier version than 5.5, upgrade them to 5.5. Read and follow all best practices when upgrading your hosts to ESXi 5.5.

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 6.5.

   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. Run vCenter Host Agent Pre-Upgrade Checker.
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. Under the **Configure** tab, click **General**.

   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.

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 determines your post-upgrade deployment type.

- If your vCenter Server 5.5 service and vCenter Single Sign-On 5.5 service are deployed on the same virtual machine or physical server, the installer upgrades them to vCenter Server 6.5 with an embedded Platform Services Controller instance. See About the vCenter Server for Windows Upgrade Process.

- If your vCenter Server 5.5 service and vCenter Single Sign-On 5.5 service are deployed on different virtual machines or physical servers, the installer upgrades them to vCenter Server 6.5 with an external Platform Services Controller instance. For information on the consolidation of distributed services during the upgrade, see Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration and Example Upgrade Paths for vCenter Server version 5.5 to version 6.5.
- If you have vCenter Server 6.0, your current deployment type is preserved during the upgrade.

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

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

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.
   - If you are upgrading from vCenter Server 5.5 to vCenter Server with 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.
   - If you are upgrading from vCenter Server 5.5 to vCenter Server with 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.
   - If you are upgrading from vCenter Server 6.0, the software preserves your current deployment during the upgrade to vCenter Server 6.5.
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 6.5 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 6.5.

   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 Confirm that no processes conflict.

8 Download the installer.

Results

Your vCenter Server environment is ready for the upgrade. See Upgrading vCenter Server 5.5 on Windows or Upgrading vCenter Server 6.0 on Windows .

Synchronizing Clocks on the vSphere Network

Verify 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.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the Knowledge Base article http://kb.vmware.com/kb/1318.

To synchronize ESXi clocks with an NTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see *vSphere Single Host Management*.

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 VMware Host Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

Procedure

1 Start the VMware Host Client, and connect to the ESXi host.

2 Click **Configure**.

3 Under **System**, click **Time Configuration**, and click **Edit**.

4 Select **Use Network Time Protocol (Enable NTP client)**.

5 In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.

6 (Optional) Set the startup policy and service status.

7 Click **OK**.

The host 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 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.

Note Starting with vSphere 6.5, the vCenter Server services are not standalone services under Windows SCM, instead they run as child processes of the VMware Service Lifecycle Manager service.

Required Information for Upgrading vCenter Server on 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.

Important vSphere supports upgrades from vCenter Server 5.5 and later to vCenter Server 6.5. To upgrade from vCenter Server 5.0 or 5.1, you must first upgrade the vCenter Server instance to version 5.5 Update 2 and then upgrade it to vCenter Server 6.5. For information about upgrading vCenter Server 5.0 or 5.1 to version 5.5, see the *VMware vSphere 5.5 Documentation*.

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 3-7. Information Required for Upgrading vCenter Server for Windows.

Required Information	Default Value	Your Entry
vCenter Single Sign-On administrator user name	administrator@vsphere.local **Important** The user must be administrator@*your_domain_name*.	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 **Important** The user must be administrator@*your_domain_name*.	
vCenter Server password		

Table 3-7. Information Required for Upgrading vCenter Server for Windows. (continued)

Required Information		Default Value	Your Entry
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 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). For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.		Join the CEIP	

Upgrading vCenter Server 5.5 on Windows

You can upgrade a vCenter Server for Windows instance with an embedded or external vCenter Single Sign-On to a vCenter Server Appliance instance with an embedded Platform Services Controller.

When you upgrade a vCenter Server instance with an embedded vCenter Single Sign-On on Windows, you upgrade the entire deployment at the same time.

Figure 3-1. vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Upgrade

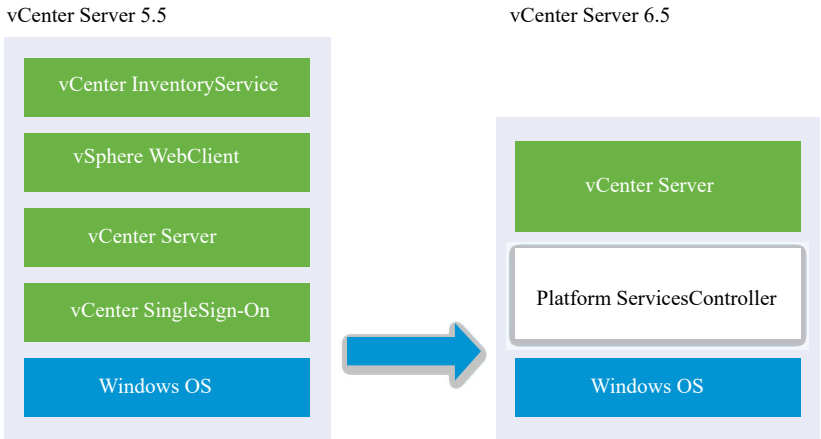
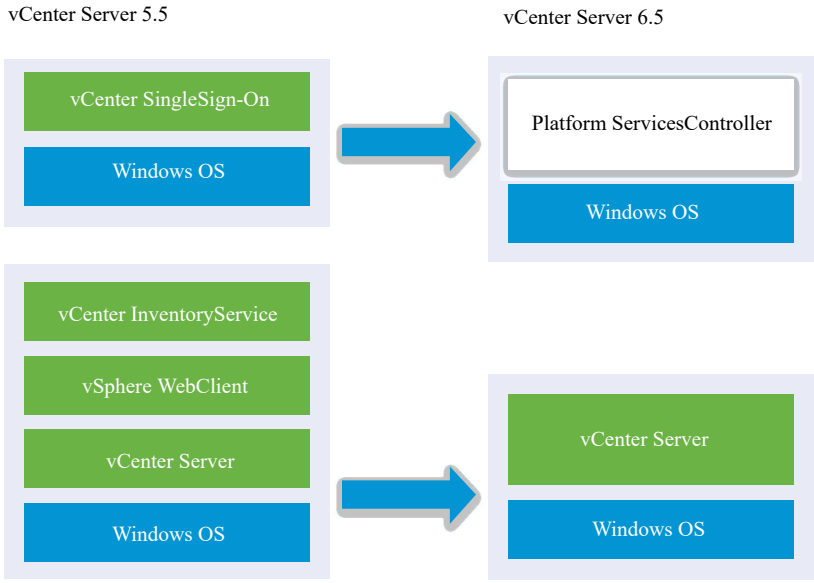


Figure 3-2. vCenter Server 5.5 with External vCenter Single Sign-On Before and After Upgrade



Upgrade tasks:

1 Download and Mount the vCenter Server Appliance Installer

2 Assemble the Required Information for Upgrading vCenter Server on Windows.

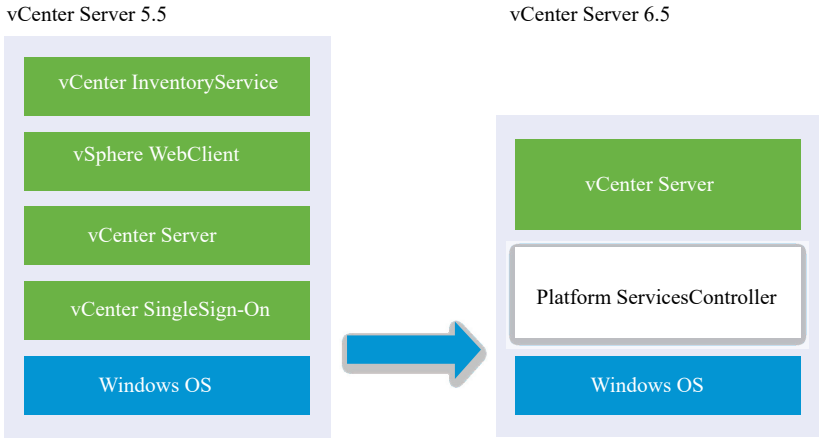
3 Upgrade a vCenter Server 5.5 Installation with an Embedded vCenter Single Sign-On or Upgrade vCenter Single Sign-On 5.5 on Windows.

Important Concurrent upgrades of vCenter Server instances with embedded vCenter Single Sign-On or Platform Services Controller are not supported. You must upgrade the instances in a sequence.

Upgrade a vCenter Server 5.5 Installation with an Embedded vCenter Single Sign-On

When you upgrade a vCenter Server instance with an embedded vCenter Single Sign-On, you upgrade the entire deployment at the same time.

Figure 3-3. vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Upgrade



- 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 Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration and Example Upgrade Paths for vCenter Server version 5.5 to version 6.5.
- 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 vCenter Server 6.5, 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.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See 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 Installer for Windows.

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 upgrade.

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 Review the Welcome page and accept the license agreement.

5 Enter your credentials.

- Enter your vCenter Server administrator credentials.
- If vCenter Single Sign-On is present, enter the administrator@vsphere.local user credential and the vCenter Single Sign-On credential.
- Click Next.

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.

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.

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.

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.

What to do next

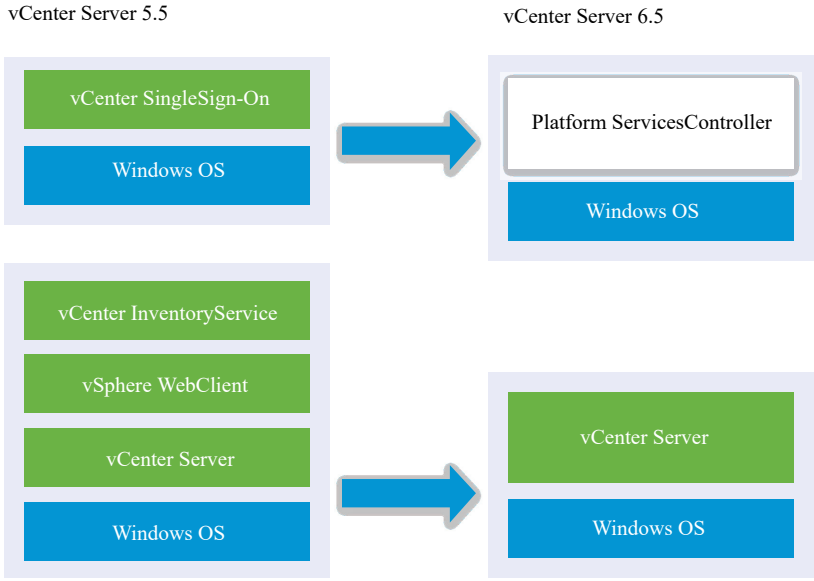
Verify that your upgrade was successful. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For information on post-upgrade steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

Upgrade vCenter Single Sign-On 5.5 on Windows

You can upgrade an externally deployed vCenter Single Sign-On 5.5 to an externally deployed Platform Services Controller 6.5 instance by using the vCenter Server for Windows installer.

Figure 3-4. vCenter Server 5.5 with External vCenter Single Sign-On Before and After Upgrade



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. For information on vCenter Server behavior in mixed version environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

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 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 Installer for Windows

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 upgrade.
3. Select vCenter Server for Windows and click Install.

   The software 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. 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.

   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.

11 Before clicking Finish, note the post upgrade steps.

12 Click Finish to complete the upgrade.

What to do next

Verify that your Platform Services Controller instance has upgraded successfully. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For the upgraded Platform Services Controller instance to replicate infrastructure data with other Platform Services Controller instances, you must migrate or upgrade all joined Platform Services Controller instances within the vCenter Single Sign-On domain to the same version. For information on migrating vCenter Single Sign-On 5.5 instances on Windows to an appliance, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance or CLI Migration of a vCenter Server Installation from Windows to an Appliance.

After you migrate or upgrade all joined Platform Services Controller instances, you can migrate or upgrade the vCenter Server instances within the vCenter Single Sign-On domain. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 5.5 on Windows. For information on migrating vCenter Server instances to appliances, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance or CLI Migration of a vCenter Server Installation from Windows to an Appliance.

Upgrade vCenter Server 5.5 on Windows

You can upgrade your vCenter Server 5.5 instance to version 6.5 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 Distributed vCenter Server 5.5 for Windows Services Relocation During Upgrade or Migration and Example Upgrade Paths for vCenter Server version 5.5 to version 6.5.
- 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 vCenter Server 6.5, 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 on Windows.

- For information on the vCenter Server upgrade process, see About the vCenter Server for Windows Upgrade Process.
- For information on vCenter Server behavior in mixed version environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.
- For information about upgrading vCenter Single Sign-On 5.5, see Upgrade vCenter Single Sign-On 5.5 on Windows.
- For information on post-upgrade steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See 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 Installer for Windows.

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 Complete the installation wizard steps and accept the license agreement.

5 Enter your credentials.

- Enter your vCenter Server administrator credentials.
- If vCenter Single Sign-On is present, enter the administrator@vsphere.local user credential and the vCenter Single Sign-On credential.
- Click Next.

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.

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.

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 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.

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

10 Click Finish to complete the upgrade.

Results

Your vCenter Server upgrade is complete. For information on post-upgrade tasks, see Chapter 5 After Upgrading or Migrating vCenter Server.

Upgrading vCenter Server 6.0 on Windows

You upgrade a vCenter Server instance with an embedded Platform Services Controller in one step. When you upgrade a vCenter Server with an external Platform Services Controller on Windows, you upgrade the instance in two steps.

1 First you upgrade the Platform Services Controller instance to version 6.5.For upgrade steps, see Upgrade vCenter Platform Services Controller 6.0 on Windows.

2 Next you upgrade the vCenter Server instance to version 6.5. For upgrade steps, see Upgrade vCenter Server 6.0 on Windows.

Figure 3-5. vCenter Server 6.0.x with Embedded Platform Services Controller Deployment Before and After Ugrade

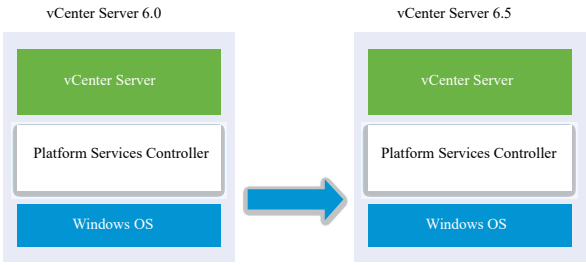
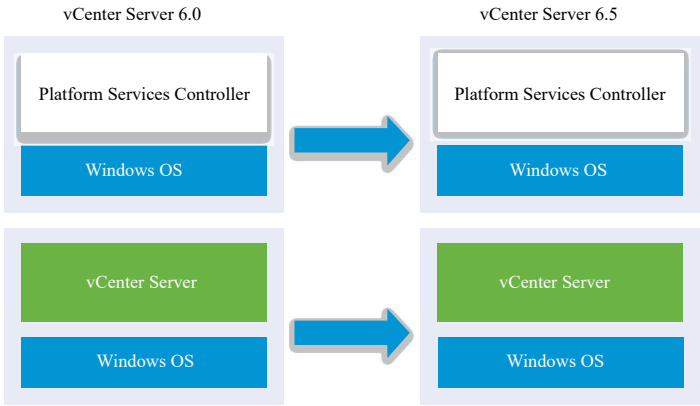


Figure 3-6. vCenter Server 6.0.x with External Platform Services Controller Before and After Upgrade



Upgrade Order

When upgrading multiple instances of vCenter Server, upgrade order matters: you upgrade all Platform Services Controller instances before upgrading vCenter Server instances. See Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Concurrent upgrades of Platform Services Controller instances are not supported. When upgrading multiple instances of vCenter Server that share the same vCenter Single Sign-On or Platform Services Controller, you can upgrade the vCenter Server instances concurrently after first upgrading the vCenter Single Sign-On or Platform Services Controller.

Mixed Platform Upgrades

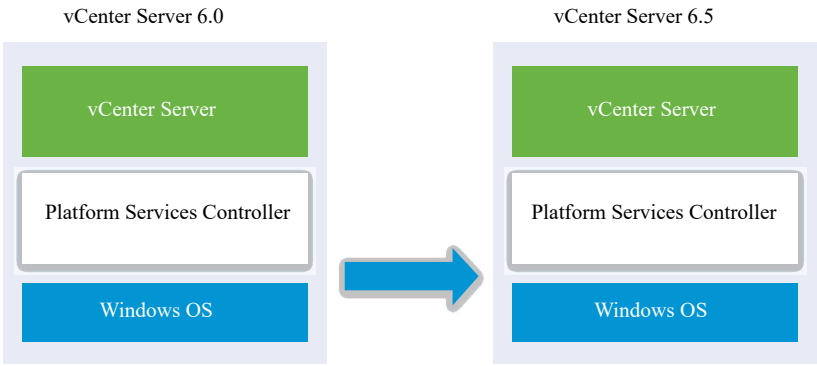
When upgrading vCenter Server instances on Windows in a mixed platform environment with a Platform Services Controller 6.0 appliance, you upgrade the Platform Services Controller appliance to version 6.5 before upgrading the vCenter Server instances. For Platform Services Controller 6.0 appliance upgrade steps, see Upgrade a Platform Services Controller Appliance 6.0 by Using the GUI.

When upgrading vCenter Server Appliance instances in a mixed platform environment with a Platform Services Controller instance on Windows, you upgrade the Platform Services Controller instance before upgrading the vCenter Server Appliance instances to version 6.5. For vCenter Server Appliance 6.0 upgrade steps, see Upgrade a vCenter Server Appliance 5.5 or 6.0 with an External vCenter Single Sign-On or Platform Services Controller Instance by Using the GUI.

Upgrade a vCenter Server 6.0 Installation with an Embedded Platform Services Controller

When you upgrade a vCenter Server instance with an embedded Platform Services Controller on Windows, you upgrade the entire deployment at the same time.

Figure 3-7. vCenter Server 6.0.x with Embedded Platform Services Controller Deployment Before and After Ugrade



- vCenter Server 6.0 ports that are in use by vCenter Server and Platform Services Controller are preserved. You cannot change ports during the upgrade. For information on required ports, see Required Ports for vCenter Server and Platform Services Controller.
- For information on vCenter Server behavior in mixed version environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See 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 be 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 Installer for Windows.

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 upgrade.
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. Review the Welcome page and accept the license agreement.
5. Enter your credentials.
   - Enter your vCenter Server administrator credentials.
   - Enter the administrator@vsphere.local user credential and the vCenter Single Sign-On credential. The user must be administrator@*your_domain_name*.
   - Click Next.

   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.
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.

   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.

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.

What to do next

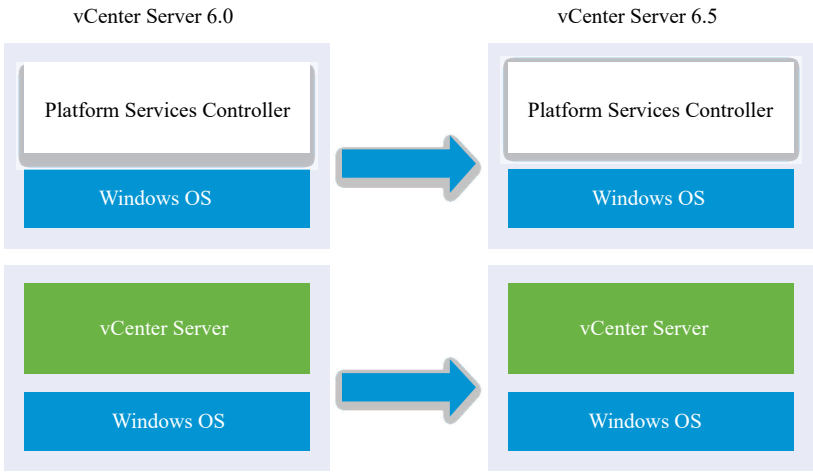
Verify that your upgrade was successful. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For information on post-upgrade steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

Upgrade vCenter Platform Services Controller 6.0 on Windows

You can upgrade your externally deployed Platform Services Controller 6.0 instance to an externally deployed Platform Services Controller 6.5 instance by using the vCenter Server for Windows installer.

Figure 3-8. vCenter Server 6.0.x with External Platform Services Controller Before and After Upgrade



In a mixed version environment, any vCenter Server 6.0 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 information on vCenter Server behavior in mixed version environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.

Prerequisites

- Your current Platform Services Controller instance is externally deployed.
- Verify your configuration meets the upgrade requirements, see vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See 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 be stopped for the vCenter Server upgrade software to uninstall Platform Services Controller during the upgrade process.
- Download the vCenter Server Installer. See Download the vCenter Server Installer for Windows

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 upgrade.
3. Select vCenter Server for Windows and click Install.

   The software 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 user must be administrator@*your_domain_name*.

   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. 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.

   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.

11 Before clicking Finish, note the post upgrade steps.

12 Click Finish to complete the upgrade.

What to do next

If you have multiple Platform Services Controller instances, you must upgrade all of them before upgrading any affiliated vCenter Server instances. After upgrading all Platform Services Controller instances to version 6.5, you can upgrade your vCenter Server instances. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 6.0 on Windows. For information on migrating vCenter Server instances to appliances, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance or CLI Migration of a vCenter Server Installation from Windows to an Appliance.

Verify that your Platform Services Controller instance has upgraded successfully. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For the upgraded Platform Services Controller instance to replicate infrastructure data with other Platform Services Controller instances, you must migrate or upgrade all joined Platform Services Controller instances within the vCenter Single Sign-On domain to the same version. For information on migrating Platform Services Controller instances on Windows to an appliance, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance or CLI Migration of a vCenter Server Installation from Windows to an Appliance.

After you migrate or upgrade all joined Platform Services Controller instances, you can migrate or upgrade the vCenter Server instances within the vCenter Single Sign-On domain. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 6.0 on Windows. For information on migrating vCenter Server instances on Windows to appliances, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance or CLI Migration of a vCenter Server Installation from Windows to an Appliance.

Upgrade vCenter Server 6.0 on Windows

You can upgrade your vCenter Server 6.0 instance to version 6.5 by using the vCenter Server for Windows installer.

The upgrade process preserves your vCenter Server 6.0 configuration.

- If your Platform Services Controller is embedded, the installer upgrades it as part of the vCenter Server upgrade.
- vCenter Server 6.0 ports that are in use by vCenter Server and Platform Services Controller 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 database that is included in vCenter Server. For information about migrating from Microsoft SQL Server Express to Microsoft SQL Server before upgrading to vCenter Server 6.5, 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 any external Platform Services Controller instances, you must upgrade them to Platform Services Controller 6.5 instances before upgrading your vCenter Server 6.0 instances to 6.5.

- For information on the vCenter Server upgrade process, see About the vCenter Server for Windows Upgrade Process.
- For information on vCenter Server behavior in mixed version environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.
- For information about upgrading Platform Services Controller 6.0, see Upgrade vCenter Platform Services Controller 6.0 on Windows.
- For information on post-upgrade steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

Prerequisites

- Verify that your configuration meets the upgrade requirements. See vCenter Server for Windows Requirements.
- Complete the preparation to upgrade tasks. See 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 Installer for Windows.

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. Review the Welcome page and accept the license agreement.
5. Enter your credentials.
   - Enter your vCenter Server administrator credentials.
   - If vCenter Single Sign-On is present, enter the administrator@vsphere.local user credential and the vCenter Single Sign-On credential. The user must be administrator@*your_domain_name*.
   - Click Next.

   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.
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.

   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 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.
9. Before clicking Finish, take note of the post upgrade steps.
10. Click Finish to complete the upgrade.

Results

Your vCenter Server upgrade is complete. For information on post-upgrade tasks, see Chapter 5 After Upgrading or Migrating vCenter Server.

Migrating vCenter Server for Windows to vCenter Server Appliance

4

You can migrate a vCenter Server installation on Windows to a vCenter Server Appliance installation while upgrading to version 6.5.

This chapter includes the following topics:

Overview of Migration from vCenter Server on Windows to an Appliance

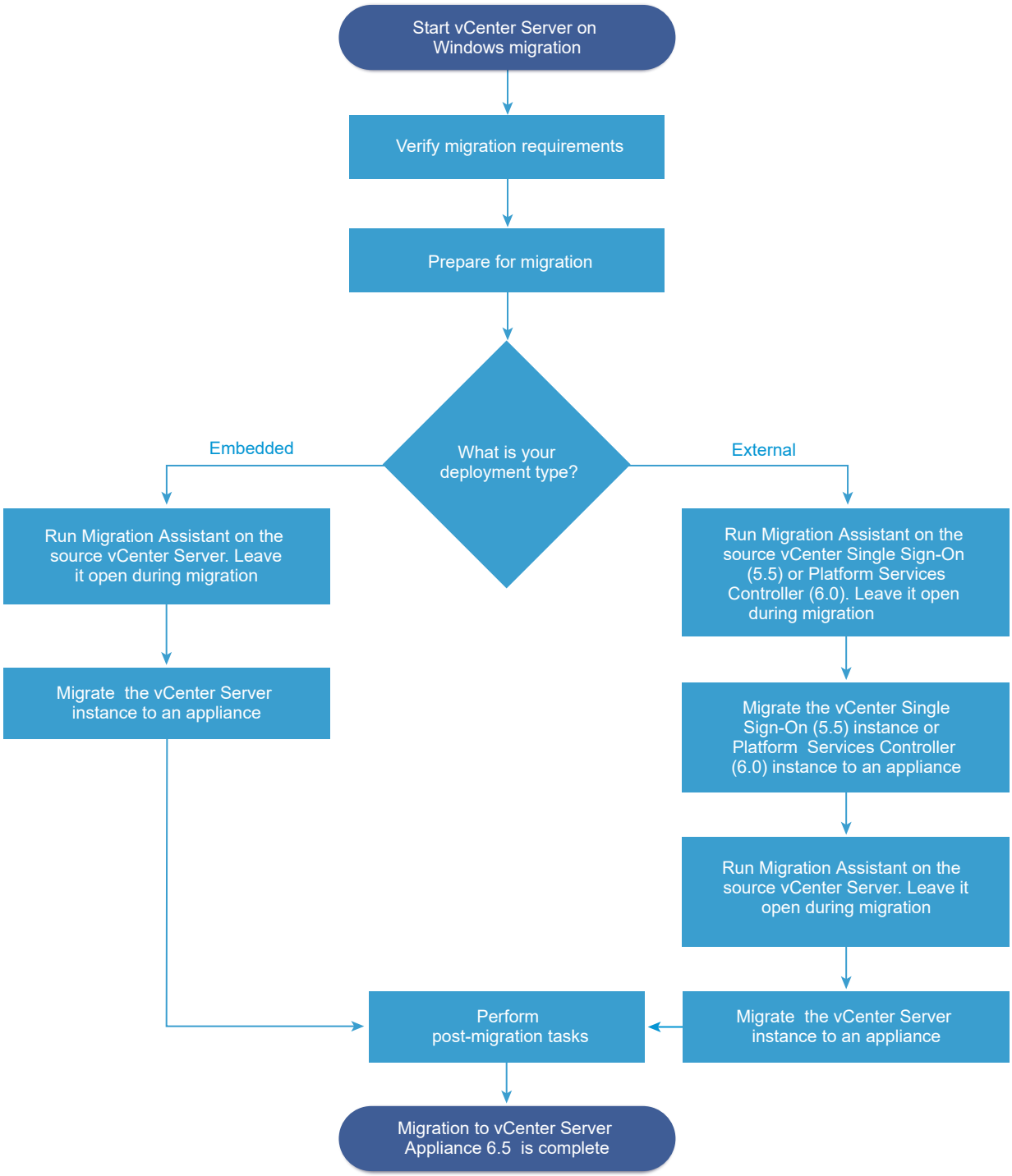
VMware provides supported paths for migrating from vCenter Server version 5.5 and version 6.0 installations on Windows to vCenter Server Appliance 6.5 installations.

You can migrate the following deployments:

Table 4-1. Supported vSphere Migration Paths

Source Configuration	Target Configuration
vCenter Server 5.5 with an embedded vCenter Single Sign-On instance on Windows	vCenter Server Appliance 6.5 with an embedded Platform Services Controller appliance
vCenter Server 6.0 with an embedded Platform Services Controller instance on Windows	
vCenter Single Sign-On 5.5 instance on Windows	External Platform Services Controller 6.5 appliance
Platform Services Controller 6.0 instance on Windows	
vCenter Server 5.5 instance on Windows	vCenter Server Appliance 6.5 with an external Platform Services Controller appliance
vCenter Server 6.0 instance on Windows	

Figure 4-1. High-level Tasks for vCenter Server on Windows Migration to vCenter Server Appliance 6.5



You can use the GUI method or the CLI method to migrate your vCenter Server installation from Windows to an appliance.

- GUI Migration of vCenter Server with an Embedded vCenter Single Sign-On or Platform Services Controller to an Appliance

- GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance
- CLI Migration of a vCenter Server Installation from Windows to an Appliance

Important You cannot change your deployment type during migration.

Migration of Update Manager from Windows to a vCenter Server Appliance 6.5

For vSphere 6.0 and earlier releases, 64-bit Windows operating systems are the only supported host operating systems for Update Manager. In vSphere 6.5, Update Manager is provided as an optional service in the vCenter Server Appliance 6.5. VMware provides supported paths for migrating Update Manager from a Windows operating system to a vCenter Server Appliance 6.5.

You can migrate Update Manager in the following vCenter Server deployments:

Table 4-2. Supported Migration Paths for Update Manager That Runs on Windows to a vCenter Server Appliance

Source Configuration	Target Configuration
vCenter Server and Update Manager run on the same Windows machine	vCenter Server Appliance 6.5 with embedded Update Manager
vCenter Server and Update Manager run on different Windows machines	vCenter Server Appliance 6.5 with embedded Update Manager
Update Manager run on a Windows machine and is connected to a vCenter Server Appliance	vCenter Server Appliance 6.5 with embedded Update Manager

You can use the GUI method or the CLI method to migrate your vCenter Server deployment that uses external Update Manager instance. If you use the GUI method, perform manual steps on the Update Manager Windows system. If you use the CLI method, add configuration parameters about Update Manager in your JSON template.

Note If you are migrating a vCenter Server system that uses an external instance of Update Manager that runs on a separate Windows machine, first run Migration Assistant on the Update Manager machine.

Important Verify that the Update Manager source machine does not run additional extensions that are connected to other vCenter Server systems, which are not part of your migration.

Before the migration, Update Manager might use any of the supported Microsoft SQL Server, or Oracle, or the Embedded database solution. After the migration to the vCenter Server Appliance, Update Manager starts to use the PostgreSQL Database.

System Requirements for Migrating vCenter Server Deployments to vCenter Server Appliance Deployments

Your source and target systems must meet specific software and hardware requirements before you can migrate a vCenter Server, vCenter Single Sign-On, or Platform Services Controller deployment to a vCenter Server Appliance or Platform Services Controller appliance.

Source System

- Your source system must meet specific software and hardware requirements for vCenter Server for Windows. See vCenter Server for Windows Requirements.
- Synchronize the clocks on all machines running the source vCenter Server services. See Synchronizing Clocks on the vSphere Network.
- Verify that your vCenter Server and Platform Services Controller certificates are valid for the vCenter Server or Platform Services Controller and have not expired.
- Verify that the system network name of the machines running the target vCenter Server services are valid, and are reachable from other machines in the network.
- Verify that the host name of the virtual machine or physical server from which you are migrating vCenter Server 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)**
  - **Replace a process level token**
- 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.
- Verify that the source vCenter Server instance or Platform Services Controller instance on Windows does not use a DHCP IP address as its system network name.

  Important Migration from a source Windows machine using a DHCP IP Address as its system network name to an appliance is not supported.

Target System

- Your target system must meet specific software and hardware requirements for vCenter Server Appliance. See System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance.
- When you use Fully Qualified Domain Names, make sure that the machine you use for deploying the vCenter Server Appliance and the target ESXi host or vCenter Server instance are on the same DNS server.
- Synchronize the clocks of all target virtual machines on the vSphere network before beginning migration. Unsynchronized clocks might result in authentication problems and can cause the migration to fail or prevent the vCenter Server services from starting. See Synchronizing Clocks on the vSphere Network.

Pre-migration Checks

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

Source Environment Checks

When you migrate vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0), vCenter Single Sign-On is included as part of the Platform Services Controller. When you provide the information about the 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 migration process.

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

- vCenter Server, Platform Services Controller, or vCenter Single Sign-On version to verify that migration is supported
- SSL certificates validity and compatibility with system names
- Network connections
- DNS resolution
- Internal and external ports used
- External database connectivity
- Administrator privileges on the Windows machine
- Required disk space for exporting configuration data
- NTP server validation
- Any credentials that you enter

Target Environment Checks

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

- Minimum processor requirements
- Minimum memory requirements
- Minimum disk space requirements
- Administrator privileges on the target host
- Any credentials that you enter

Known Limitations

The current release has several known limitations.

The following list contains features or actions that are currently not supported:

- Local Windows OS users and groups are not migrated to the Photon OS of the vCenter Server Appliance 6.5. If you assigned vCenter Server permissions to any Local Windows OS users and groups, remove the permissions assignments before the migration. You can re-create Local OS users and groups on the Photon OS of the vCenter Server Appliance 6.5 after the migration.
- After the migration, the source vCenter Server is turned off and cannot be turned on to avoid network ID conflicts with the target vCenter Server Appliance. After the source vCenter Server is turned off, all solutions that are installed on the source vCenter Server and that are not migrated become unavailable.
- Migration of deployments that use custom ports for services other than Auto Deploy, HTTP and HTTPS, Update Manager, and vSphere ESXi Dump Collector are not supported.
- The migration process migrates only one network adapter settings to the target vCenter Server Appliance. If the hostname of the source vCenter Server resolves to multiple IP addresses across multiple network adapters, you have the option to select which IP address and network adapter settings to migrate. You cannot add the rest of the network adapters and settings to the target vCenter Server Appliance.
- You cannot migrate a vCenter Server instance that uses a DHCP IP address.

Preparing for Migration

Before beginning to migrate any type of vCenter Server deployment to an appliance, you must complete the preparation tasks.

Preparation tasks:

- Synchronizing Clocks on the vSphere Network
- Preparing vCenter Server Databases for Migration

- Preparing to Migrate the Content Library
- Prepare Managed ESXi Hosts for Migration
- Download and Mount the vCenter Server Appliance Installer
- Download and Run VMware Migration Assistant on the Source Windows Machine

Synchronizing Clocks on the vSphere Network

Verify 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.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the Knowledge Base article http://kb.vmware.com/kb/1318.

To synchronize ESXi clocks with an NTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see *vSphere Single Host Management*.

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 VMware Host Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

Procedure

1. Start the VMware Host Client, and connect to the ESXi host.
2. Click **Configure**.
3. Under **System**, click **Time Configuration**, and click **Edit**.
4. Select **Use Network Time Protocol (Enable NTP client)**.
5. In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.
6. (Optional) Set the startup policy and service status.
7. Click **OK**.

   The host synchronizes with the NTP server.

Preparing vCenter Server Databases for Migration

The vCenter Server Appliance instance requires a database to store and organize server data. Ensure your source vCenter Server database is prepared for migration to the target vCenter Server Appliance.

Each vCenter Server Appliance instance must have its own database. The bundled PostgreSQL database that is included in the vCenter Server Appliance supports up to 2,000 hosts and 35,000 virtual machines.

To ensure your database is prepared for migration:

- Verify that passwords are current and not set to expire soon.
- (Optional) Reduce the database size. For more information, see http://kb.vmware.com/kb/2110031.
- For vCenter Server 5.5, run the cleanup scripts to remove any unnecessary data in the vCenter Server database using the steps for your database. For details see:
  - Prepare an Oracle Database for Migration,
  - Prepare a Microsoft SQL Server Database for Migration
  - Prepare PostgreSQL Database Before Migrating vCenter Server to an Appliance
- Verify that you have backed up your database. See your database documentation.
- Verify that vCenter Server can communicate with the local database. See Verify That vCenter Server Can Communicate with the Local Database.

During the migration of vCenter Server to vCenter Server Appliance, the installer:

1. Exports the vCenter Server database.
2. Deploys the target vCenter Server Appliance in an unconfigured state.
3. Copies exported data to the target vCenter Server Appliance.
4. Starts the PostgreSQL service to import the source database data.
5. Upgrades the database schema to be compatible with the target vCenter Server Appliance.
6. Starts the target vCenter Server Appliance services.

When you configure the target vCenter Server Appliance, you initialize and configure using the imported database with the old schema. You have a choice of migration options:

1. Inventory tables
2. Inventory tables with events and tasks
3. All database data

Prepare an Oracle Database for Migration

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your Oracle database from Windows to an embedded PostgreSQL database in the appliance.

Prerequisites

Verify that you have confirmed basic interoperability before preparing your Oracle database for migration.

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

Procedure

1. Verify that passwords are current and not set to expire soon.
2. 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.
3. 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.
4. Verify that the JDBC driver file is included in the CLASSPATH variable.
5. Verify that permissions are set correctly.
6. Either assign the DBA role or grant the required permissions to the user.
7. For vCenter Server 5.5, run the cleanup script.
   a. Locate the cleanup_orphaned_data_Oracle.sql script in the ISO image and copy it to the Oracle server.

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

   c. Run the cleanup script.

      `@path/cleanup_orphaned_data_Oracle.sql`

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

8 Make a full backup of the vCenter Server database.

Results

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Prepare a Microsoft SQL Server Database for Migration

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your Microsoft SQL Server database on Windows to an embedded PostgreSQL database appliance.

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

Procedure

1 Verify that passwords are current and not set to expire soon.

2 Verify that JDK 1.6 or later is installed on the vCenter Server machine.

3 Verify that the `sqljdbc4.jar` file is added to the CLASSPATH variable on the machine where vCenter Server Appliance is to be migrated.

   If the `sqljdbc4.jar` file is not installed on your system, the vCenter Server Appliance installer installs it.

4 Verify that your system database source name is using the Microsoft SQL Server Native Client 10 or 11 driver.

5 For vCenter Server 5.5, run the cleanup script.

   a Locate the `cleanup_orphaned_data_MSSQL.sql` script in the ISO image and copy it to a location accessible by the Microsoft SQL server.

   b Log in to your database.

   - For Microsoft SQL Server Express, open a command prompt.
   - For Microsoft SQL Server, log in to a Microsoft SQL Server Management Studio session as the vCenter Server database user.

   c Run the cleanup script.

   For Microsoft SQL Server Express, run: **`sqlcmd -E -S localhost\VIM_SQLEXP -d VIM_VCDB -i path/cleanup_orphaned_data_MSSQL.sql`**
   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.

6 Make a full backup of the vCenter Server database.

Results

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Prepare PostgreSQL Database Before Migrating vCenter Server to an Appliance

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your PostgreSQL database installation on Windows to an appliance.

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

Prerequisites

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

Procedure

1 Verify that passwords are current and not set to expire soon.

2 For vCenter Server, 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/vpostgres/9.4/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.

Results

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Preparing to Migrate the Content Library

When migrating from vCenter Server version 6.0 or earlier, you must prepare your environment before migrating the Content Library to prevent pre-check errors.

- All ESXi hosts from the source vCenter Server inventory must be supported by the destination vCenter Server 6.5.
- The source vCenter Server Content Libraries must be backed by either remote file system or datastores . You cannot use libraries backed by the local file system of the vCenter Server.

- All the remote file system shares used as library backings must be accessible at the time of the migration.
- No subscribed libraries are using file-based subscription URI.

If you are migrating from vCenter Server 6.0 U1, no actions are necessary.

The migration will fail, if your environment does not meet the requirements..

Prepare Managed ESXi Hosts for Migration

You must prepare the ESXi hosts that are managed by your vCenter Server installation before migrating it from Windows to an appliance.

Prerequisites

To migrate vCenter Server, vCenter Single Sign-On, or Platform Services Controller from Windows to an appliance, your source and target ESXi hosts must meet the migration requirements.

- ESXi hosts must be at version 5.5 or greater. If your ESXi hosts are at an earlier version than 5.5, upgrade them to 5.5. Read and follow all best practices when upgrading your hosts to ESXi 5.5.
- 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 6.5.

   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.

Preparing vCenter Server Certificates for Migration

You must verify that your source vCenter Server certificates are prepared before you start the migration process.

The instructions apply to vCenter Server 5.5 source deployments.

In vSphere 6.0 and later certificates are stored in the VMware Endpoint Certificate Store. The migration process proceeds normally and preserves your certificates. For information about vCenter Server 6.0 certificates location, see http://kb.vmware.com/kb/2111411

Certificate Files Location

The vCenter Server certificate files are located at `%ProgramData%\VMware\VMware VirtualCenter\SSL`

Supported Certificate Types

If your environment uses any of the supported certificate types, you can continue with the migration. The migration process proceeds normally and preserves your certificates.

- Your `rui.crt` file contains the entire chain including the leaf certificate. You can create this type of certificate by deploying and using the VMware SSL Certificate Automation Tool, see http://kb.vmware.com/kb/2057340.
- Your `rui.crt` file contains the leaf certificate and the corresponding `cacert.pem` is available in `%ProgramData%\VMware\VMware VirtualCenter\SSL` to validate the `rui.crt`.

Unsupported Certificate Types

If your environment uses any of the unsupported certificate types, you must prepare your certificates before you can proceed with the migration process proceeds.

- Your `rui.crt` contains only the leaf certificate, the `cacert.pem` is missing or invalid, and `cacert.pem` is not added to the Windows trust store.

  Get the Certificate Authority certificate, including all intermediate certificates, and create a `cacert.pem` file, or replace the vCenter Server certificates with any of the supported formats.

- Your `rui.crt` contains only the leaf certificate and the `cacert.pem` is missing or invalid, but the `cacert.pem` is added to the Windows trust store.

  Get the Certificate Authority certificate, including all intermediate certificates from the Windows trust store and create `cacert.pem`. Use OpenSSL to verify the certificate by running `verify -CAfile cacert.pem rui.crt` command.

For more information about vSphere security certificates, see the *vSphere Security* documentation.

System Requirements for the vCenter Server Appliance Installer

You can run the vCenter Server Appliance GUI or CLI installer from a network client machine that is running on a Windows, Linux, or Mac operating system of a supported version.

To ensure optimal performance of the GUI and CLI installers, use a client machine that meets the minimum hardware requirements.

Table 4-3. System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	■ Windows 7, 8, 8.1, 10 ■ Windows 2012 x64 bit ■ Windows 2012 R2 x64 bit ■ Windows 2016 x64 bit	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	■ SUSE 12 ■ Ubuntu 14.04	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC **Note** The CLI installer requires 64-bit OS.
Mac	■ macOS v10.9, 10,10, 10.11 ■ macOS Sierra	8 GB RAM, 1 CPU having 4 cores with 2.4 GHz, 150 GB hard disk, 1 NIC

Note For client machines that run on Mac 10.11, concurrent GUI deployments of multiple appliances are unsupported. You must deploy the appliances in a sequence.

Determine the Oracle Database Size and the Storage Size for the New Appliance

Before upgrading a vCenter Server Appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new appliance so that the embedded PostgreSQL database can successfully assume the data from the old database with enough free disk space after the upgrade.

You run scripts to determine the Oracle core table size, the events and tasks table size, and the statistics table size. The Oracle core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Oracle events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Oracle tables size.

During the upgrade of the appliance, you can select the types of data to transfer to the new appliance. For minimum upgrade time and storage requirement for the new appliance, you can select to transfer only the configuration data.

Prerequisites

You must have the vCenter Server database login credentials.

Procedure

1 Log in to a SQL*Plus session with the vCenter Server database user.

2 Determine the core table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
  FROM   user_segments s
  WHERE  (s.segment_name,s.segment_type)
                IN (SELECT seg_name, seg_type FROM
                         (SELECT t.table_name seg_name, t.table_name tname,
                           'TABLE' seg_type
                           FROM   user_tables t
                          UNION
                          SELECT i.index_name, i.table_name,
                          'INDEX'
                           FROM   user_indexes i
                         ) ti
                    WHERE  (ti.tname LIKE 'VPX_%'
                            OR ti.tname LIKE 'CL_%'
                            OR ti.tname LIKE 'VDC_%')
                        AND ti.tname NOT LIKE 'VPX_SAMPLE_TIME%'
                        AND ti.tname NOT LIKE 'VPX_HIST_STAT%'
                        AND ti.tname NOT LIKE 'VPX_TOPN%'
                        AND ti.tname NOT LIKE 'VPX_SDRS_STATS_VM%'
                        AND ti.tname NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
                        AND ti.tname NOT LIKE 'VPX_TASK%'
                        AND ti.tname NOT LIKE 'VPX_EVENT%'
                        AND ti.tname NOT LIKE 'VPX_PROPERTY_BULLETIN%');
```

The script returns the database storage size in MB.

3 Determine the events and tasks table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                WHERE
                   ti.tname LIKE 'VPX_TASK%'
                OR ti.tname LIKE 'VPX_EVENT%');
```

The script returns the events and tasks storage size in MB.

4 Determine the statistics table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                  WHERE
                     ti.tname LIKE 'VPX_SAMPLE_TIME%'
                  OR ti.tname LIKE 'VPX_TOPN%'
                  OR ti.tname LIKE 'VPX_TASK%'
                  OR ti.tname LIKE 'VPX_EVENT%'
                  OR ti.tname LIKE 'VPX_HIST_STAT%');
```

The script returns the statistics storage size in MB.

5 Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.

a The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Oracle core table returned in Step 2.

b The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Oracle events and tasks and statistics tables returned in Step 3 and Step 4.

For example, if the Oracle core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Determine the Microsoft SQL Server Database Size and the Storage Size for the New Appliance

Before upgrading a vCenter Server Appliance or migrating a vCenter Server on Windows that uses an external Microsoft SQL Server database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new appliance so that the embedded PostgreSQL database can successfully assume the data from the old database with enough free disk space after the upgrade.

You run scripts to determine the Microsoft SQL Server core table size, the events and tasks table size, and the statistics table size. The Microsoft SQL Server core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Microsoft SQL Server events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Microsoft SQL Server tables size.

Prerequisites

You must have the vCenter Server database login credentials.

Procedure

1 Log in to a SQL Management Studio session with the vCenter Server database user.

2 Determine the core table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
  FROM sys.dm_db_partition_stats p
  JOIN sys.objects o
    ON o.object_id = p.object_id
 WHERE o.type_desc = 'USER_TABLE'
   AND o.is_ms_shipped = 0 AND UPPER(o.name) NOT LIKE 'VPX_HIST_STAT%'
   AND UPPER(o.name) NOT LIKE 'VPX_SAMPLE_TIME%'
   AND UPPER(o.name) NOT LIKE 'VPX_TOPN%'
   AND UPPER(o.name) NOT LIKE 'VPX_TASK%'
   AND UPPER(o.name) NOT LIKE 'VPX_EVENT%'
   AND UPPER(o.name) NOT LIKE 'VPX_SDRS_STATS_VM%'
   AND UPPER(o.name) NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
   AND UPPER(o.name) NOT LIKE 'VPX_PROPERTY_BULLETIN%';
```

The script returns the database storage size in MB.

3 Determine the events and tasks table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
  FROM sys.dm_db_partition_stats p
  JOIN sys.objects o
    ON o.object_id = p.object_id
 WHERE o.type_desc = 'USER_TABLE'
   AND o.is_ms_shipped = 0 AND ( UPPER(o.name) LIKE 'VPX_TASK%'
    OR UPPER(o.name) LIKE 'VPX_EVENT%');
```

The script returns the events and tasks storage size in MB.

4 Determine the statistics table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
  FROM sys.dm_db_partition_stats p
  JOIN sys.objects o
    ON o.object_id = p.object_id
 WHERE o.type_desc = 'USER_TABLE'
   AND o.is_ms_shipped = 0
   AND (     UPPER(o.name) LIKE 'VPX_HIST_STAT%'
         OR UPPER(o.name) LIKE 'VPX_SAMPLE_TIME%'
         OR UPPER(o.name) LIKE 'VPX_TOPN%');
```

The script returns the statistics storage size in MB.

5 Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.

   a The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Microsoft SQL Server core table returned in Step 2.

   b The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Microsoft SQL Server events and tasks and statistics tables returned in Step 3 and Step 4.

   For example, if the Microsoft SQL Server core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Download and Run VMware Migration Assistant on the Source Windows Machine

You must download and run the VMware Migration Assistant on your source vCenter Server, vCenter Single Sign-On, or Platform Services Controller to prepare it for migration from Windows to an appliance. If you are using a deployment of vCenter Server with an external Update Manager that runs on Windows, download and run the VMware Migration Assistant on the source Windows machine where Update Manager runs to prepare Update Manager server and database for migration from Windows to the vCenter Server Appliance.

The VMware Migration Assistant performs the following tasks on the source Windows machine where you run it:

1 Discovers the source deployment type.

2 Runs pre-checks on the source.

3 Reports errors that must be addressed before starting the migration.

4 Provides information for the next steps in the migration process.

Ensure that the VMware Migration Assistant window remains open during the migration process. Closing the VMware Migration Assistant causes the migration process to stop.

Prerequisites

- Download and Mount the vCenter Server Appliance Installer.
- Log in to the Windows machine as an administrator.

Procedure

1 In the vCenter Server Appliance installer package, locate the directory that contains VMware Migration Assistant.

2 Copy the VMware Migration Assistant folder to the source Windows machine where either one of the following components runs:

- Update Manager
- vCenter Single Sign-On
- Platform Services Controller
- vCenter Server

Caution If Update Manager runs on a different Windows machine than any other of the vCenter Server components that you are migrating, run VMware Migration Assistant on the Update Manager source machine first. If you do not run VMware Migration Assistant on the Update Manager source machine first, the vCenter Server migration might fail.

3 Run the VMware Migration Assistant on the Windows machine.

- For the GUI, double-click `VMware-Migration-Assistant.exe`
- For the CLI, enter: **`VMware-Migration-Assistant.exe -p <password of Administrator@vmdir.domain>`**

  To list all the available input parameters, enter: **`VMware-Migration-Assistant.exe --help`**.

Important Leave the Migration Assistant window open until you complete the upgrade or the migration process of your vCenter Server deployment.

The VMware Migration Assistant runs pre-upgrade checks and prompts you to resolve any errors it finds before proceeding with the migration.

Results

When the pre-checks are finished and any errors are addressed, your source system is ready for migration.

What to do next

Follow the VMware Migration Assistant instructions to start migration.

For detailed migration steps, see one of the following.

- GUI Migration of vCenter Server with an Embedded vCenter Single Sign-On or Platform Services Controller to an Appliance
- GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance
- CLI Migration of a vCenter Server Installation from Windows to an Appliance

Prerequisites for Migrating vCenter Server and Platform Services Controller

To ensure the successful migration of the vCenter Server and Platform Services Controller, you must preform some required tasks and pre-checks before running the migration.

General Prerequisites

- Download and Mount the vCenter Server Appliance Installer.
- Verify that the clocks of all machines on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the New vCenter Server Appliance and Platform Services Controller Appliance.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not part of a fully automated DRS cluster.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster is not fully automated.

Source System Prerequisites

- Verify that the source machine that you want to migrate does not run on an ESXi host that is part of a fully automated DRS cluster.
- If you are migrating vCenter Server 5.5 and you have changed its host name, verify that the SSL certificate is configured correctly. For information about how to troubleshoot an error when you changed the vCenter Server 5.5 host name, see *vSphere Troubleshooting* in the *VMware vSphere 5.5 Documentation*.
- Verify that you have sufficient disk space on the source machine that you want to migrate so that you can accommodate the data for the migration.

- Create an image-based backup of the vCenter Server appliance you are migrating as a precaution in case there is a failure during the migration process. If you are migrating a vCenter Server appliance with an external Platform Services Controller, take a image-based backup of the Platform Services Controller appliance as well.

  Important To take a pre-migration image-based backup, power off all the vCenter Server and Platform Services Controller nodes in your environment, and take a backup of each node. After you have taken backups of all the nodes, you can restart them and proceed with the migration procedure.

  If the upgrade fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server and Platform Services Controller nodes from their respective backups. You must restore all the nodes in the environment from their backups. Failing to do so will cause the replication partners to be out of synchronization with the restored node.

  To learn about image-based back, see "Image-Based Backup and Restore of a vCenter Server Environment" in *vCenter Server Installation and Setup*.

- If you use an external database, back up the external database.

Network Prerequisites

- If you plan to assign a static IP address in the temporary network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you plan to assign a DHCP IP address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is in the same network as the ESXi host on which the existing vCenter Server Appliance runs.
- If you plan to assign a DHCP IPv4 address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is connected to at least one network that is associated with a port group which accepts MAC address changes. Note that the default security policy of a distributed virtual switch is to reject MAC address changes. For information about how to configure the security policy for a switch or port group, see *vSphere Networking*.
- Add the source vCenter Server IP address in the DNS records.

Required Information for Migrating vCenter Server from Windows to an Appliance

The vCenter Server migration wizard prompts you for the deployment and migration information when migrating a vCenter Server instance, a vCenter Single Sign-On instance, or a Platform Services Controller instance from Windows to an appliance. It is a best practice to keep a record of the values that you entered in case you must power off the appliance and restore the source installation.

You can use this worksheet to record the information that you need for migrating a vCenter Server instance with an vCenter Single Sign-On or Platform Services Controller from Windows to an appliance.

Important The user name that you use to log in to the machine from which you want run the GUI installer, the path to the vCenter Server Appliance installer, and your values including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Local OS users existing on source windows machine are not migrated to the target vCenter Server Appliance and must be recreated after migration is complete. If any local OS user names are used to log in to the vCenter Single Sign-On, you must recreate them and reassign permissions in the Platform Services Controller appliance.
If the source vCenter Server machine is joined to an Active Directory domain, the account you use must have permissions to rejoin the machine to the domain. For more information, see http://kb.vmware.com/kb/2146454.

Table 4-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance

Required Information		Default Value	Your Entry
Required source vCenter Server migration data	vCenter Server IP address or FQDN		
	vCenter Single Sign-On administrator user name	administrator@vsphere.local **Important** The user must be administrator@*your_domain_name*.	
	Password of the vCenter Single Sign-On administrator		
	Migration Assistant port number		
	vCenter Server version		
	Temporary upgrade files path	`%LOCALAPPDATA%\VMware\Migration-Assistant\export`	
	IP address or FQDN of the source ESXi host on which the source vCenter Server resides		
	Source ESXi host user name with administrative rights on the source ESXi host		
	Source ESXi host password		
	Migrate performance & other historical data	Disabled by default	

Table 4-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (continued)

Required Information		Default Value	Your Entry
	Migration Assistant thumbprint		
	Active Directory administrator credentials		
	Service account credentials, if vCenter Server is running under a customer user account		
Required target vCenter Server Appliance data	IP address or FQDN of the target ESXi host or vCenter Server instance where you deploy the new vCenter Server Appliance to which you migrate the source vCenter Server		
	User name with administrative privileges for the target ESXi host. or vCenter Server instance, data center or data center folder, and resource pool of an ESXi host or DRS cluster to which to migrate the source installation		
	Password for the target ESXi host. or vCenter Server instance, data center or data center folder, and resource pool of an ESXi host or DRS cluster		
	vCenter Single Sign-On username		
	vCenter Single Sign-On password		
	Target vCenter Server Appliance name		
	Password of the root user		
	vCenter Server Appliance size. The options vary depending on the size of your vSphere environment. ■ Tiny (up to 10 hosts, 100 virtual machines) ■ Small (up to 100 hosts, 1,000 virtual machines) ■ Medium (up to 400 hosts, 4,000 virtual machines) ■ Large (up to 1,000 hosts, 10,000 virtual machines) ■ X-Large (up to 2,000 hosts, 35,000 virtual machines)	Tiny (up to 10 hosts, 100 virtual machines)	

Table 4-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (continued)

Required Information		Default Value	Your Entry
	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	
	Join or do not participate in the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.	Join the CEIP	
Temporary network for communication between the source vCenter Server and the target 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		
Enable or disable SSH		Disabled by default	

GUI Migration of vCenter Server with an Embedded vCenter Single Sign-On or Platform Services Controller to an Appliance

You can use the GUI method to migrate a vCenter Server instance with an embedded vCenter Single Sign-On or Platform Services Controller to a vCenter Server Appliance with an embedded Platform Services Controller appliance.

When you migrate from vCenter Server with an embedded vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) on Windows to vCenter Server Appliance with an embedded Platform Services Controller appliance, the entire deployment is migrated at only one step.

If you use Update Manager in the vCenter Server deployment on Windows that you migrate, and Update Manager runs on a separate machine from any other of the vCenter Server components, take an extra step to migrate Update Manager to an appliance.

1 If your vCenter Server deployment on Windows uses an external Update Manager, run Migration Assistant on the Update Manager machine to start the migration of the Update Manager server and database to the vCenter Server Appliance.

2 Migrate the vCenter Server instance with Embedded vCenter Single Sign-On or Embedded Platform Services Controller from Windows to an appliance.

Figure 4-2. vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Migration

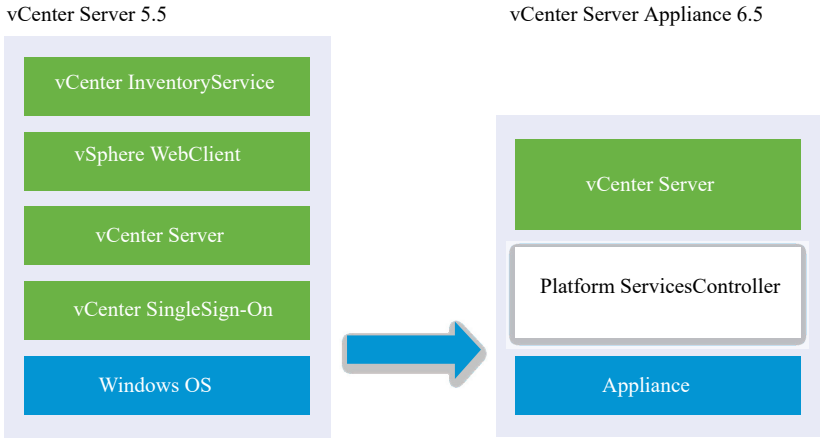
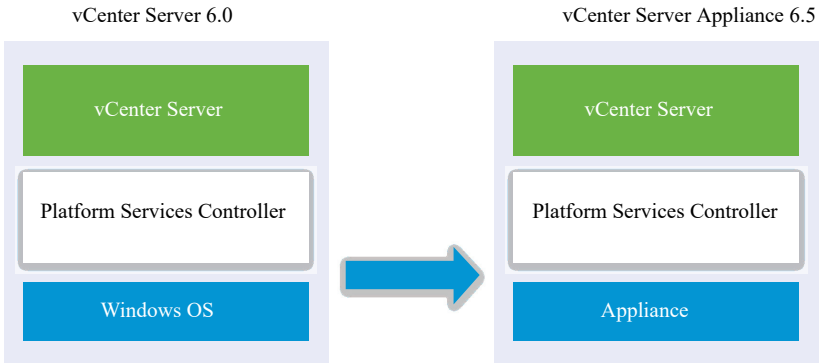


Figure 4-3. vCenter Server 6.0.x with Embedded Platform Services Controller Deployment Before and After Migration



GUI tasks for migrating vCenter Server with an embedded vCenter Single Sign-On or Platform Services Controller from Windows to an appliance:

1 Download and Mount the vCenter Server Appliance Installer ISO file on a network virtual machine or physical server from which you want to perform the migration.

2 Download and Run VMware Migration Assistant on the Source Windows Machine.

Note If you are migrating a vCenter Server system that uses an external instance of Update Manager that runs on a separate Windows machine, first run Migration Assistant on the Update Manager machine.

3 Assemble the Required Information for Migrating vCenter Server from Windows to an Appliance.

4 Deploy the OVA File for Migrating to the Target vCenter Server Appliance with an Embedded Platform Services Controller.

5 Set Up the Target vCenter Server Appliance with an Embedded Platform Services Controller

Important The user name that you use to log in to the machine from which you want run the GUI installer, the path to the vCenter Server Appliance installer, and your values including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

The installer:

- Deploys a new target appliance.
- Exports the required files from the source vCenter Server.
- Copies the required files to the new vCenter Server Appliance.
- Runs the migration process on the new vCenter Server Appliance as specified in the Summary.
- Imports and updates the files and settings of the source vCenter Server installation to the new vCenter Server Appliance.

Deploy the OVA File for Migrating to the Target vCenter Server Appliance with an Embedded Platform Services Controller

To start the migration process, you use the GUI installer to deploy the OVA file that is included in the installer ISO file as the target vCenter Server Appliance with an embedded Platform Services Controller.

Figure 4-4. vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Migration

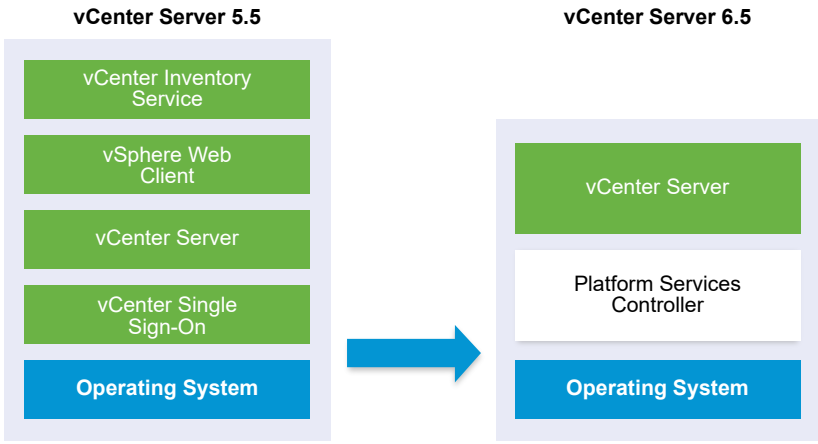
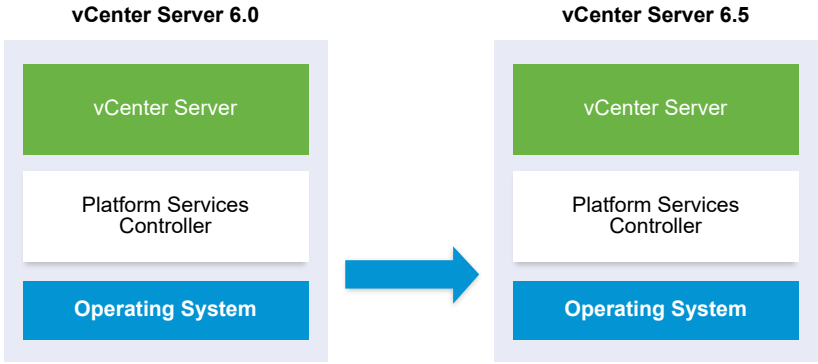


Figure 4-5. vCenter Server 6.0.x with Embedded Platform Services Controller Deployment Before and After Migration



Prerequisites

- See Prerequisites for Migrating vCenter Server and Platform Services Controller

Procedure

1. In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Migrate**.
3. Review the Introduction page to understand the migration process and click **Next**.
4. Read and accept the license agreement, and click **Next**.

5 Connect to the target server to which you want to migrate the source vCenter Server.

Option	Steps
You can connect to an ESXi host on which to deploy the target appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the target appliance.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

6 (Optional) Review the warning message and try to resolve the warnings, if any, and click **Yes**.

7 On the Set up target appliance VM page, enter a name for the target vCenter Server Appliance, set the password for the root user, and click **Next**.

The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sigh (@), or brackets (()).

Important The local operating system password is not migrated to the target appliance.

8 On the Connect to source page, enter the details for the source vCenter Server instance, and click **Next**.

a Enter the IP address or FQDN.

b Enter the user name and password of a user who has administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user.

c Enter the Migration Assistant Port you received in the Migration Assistant instructions.

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

10 Select the deployment size for the new vCenter Server Appliance for your vSphere inventory.

Note You cannot select a deployment size that is smaller than the source deployment.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 CPUs and 10 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 16 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 24 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 32 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 48 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines

Note At the bottom of the deployment size table, a row shows the size information of the source machine. This size information is reported by the migration assistant and might help understand why you cannot select some deployment sizes.

11 Select the storage size for the new vCenter Server Appliance, and click **Next**.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 250 GB of storage.	Deploys an appliance with 290 GB of storage.	Deploys an appliance with 425 GB of storage.	Deploys an appliance with 640 GB of storage.	Deploys an appliance with 980 GB of storage.
Large	Deploys an appliance with 775 GB of storage.	Deploys an appliance with 820 GB of storage.	Deploys an appliance with 925 GB of storage.	Deploys an appliance with 990 GB of storage.	Deploys an appliance with 1030 GB of storage.
X-Large	Deploys an appliance with 1650 GB of storage.	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1805 GB of storage.	Deploys an appliance with 1870 GB of storage.	Deploys an appliance with 1910 GB of storage.

12 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

13 Configure the temporary network for communication between the source vCenter Server and the target vCenter Server Appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment.

14 On the Ready to complete stage 1 page, review the deployment settings for the target vCenter Server Appliance and click **Finish** to start the OVA deployment process.

15 Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the target appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the Appliance Management Interface of the newly deployed target vCenter Server Appliance to transfer the data from the source vCenter Server and set up the services.

Results

The newly deployed target vCenter Server Appliance 6.5 with an embedded Platform Services Controller is running on the target server but is not configured.

Important The data from the source vCenter Server is not yet transferred and the services of the target appliance are not started.

Set Up the Target vCenter Server Appliance with an Embedded Platform Services Controller

When the OVA deployment completes, you are redirected to stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the newly deployed vCenter Server Appliance 6.5 with an embedded Platform Services Controller.

Your window of downtime does not begin until you begin to set up the target appliance. You cannot cancel or interrupt the process until it completes with the shut down of the source deployment. Your window of downtime ends when the target appliance starts.

Procedure

1. Review the introduction to stage 2 of the migration process and click **Next**.
2. On the Select source vCenter Server page, enter the vCenter Single Sign-On administrator password and the root password of the source vCenter Server, enter the password of the user with administrative privileges on the vCenter Server instance, and click **Next**.
3. (Optional) Accept the warning message, if any, by clicking **Yes**.
4. If your source Windows machine is connected to an Active Directory domain, enter the credentials for an administrator domain user with permission to add the target machine to the Active Directory domain, and click **Next**.

   Note The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
5. 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*.
6. On the ready to complete page, review the migration settings, accept the backup acknowledgment, and click **Finish**.
7. Click **OK** to confirm the shutdown of the source vCenter Server.
8. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

Results

The source vCenter Server instance is migrated from Windows to an appliance. The sourcevCenter Server instance is powered off and the new target appliance starts.

What to do next

Verify that your migration to an appliance was successful. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful. For post-migration steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance

You can use the GUI to migrate vCenter Server with an external vCenter Single Sign-On or Platform Services Controller to an appliance.

When you migrate from vCenter Server with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) on Windows to vCenter Server Appliance with an external Platform Services Controller appliance, you migrate in two steps.

If you use Update Manager in the vCenter Server deployment on Windows that you migrate, and Update Manager runs on a separate machine from any other of the vCenter Server components, take an extra step to migrate Update Manager to an appliance.

1. If your vCenter Server deployment on Windows uses an external Update Manager, run Migration Assistant on the Update Manager machine to start the migration of the Update Manager server and database to the vCenter Server Appliance.
2. Migrate the vCenter Single Sign-On instance or Platform Services Controller instance from Windows to an appliance.
3. Migrate the vCenter Server instance from Windows to an appliance.

Figure 4-6. vCenter Server 5.5 with External vCenter Single Sign-On Before and After Migration

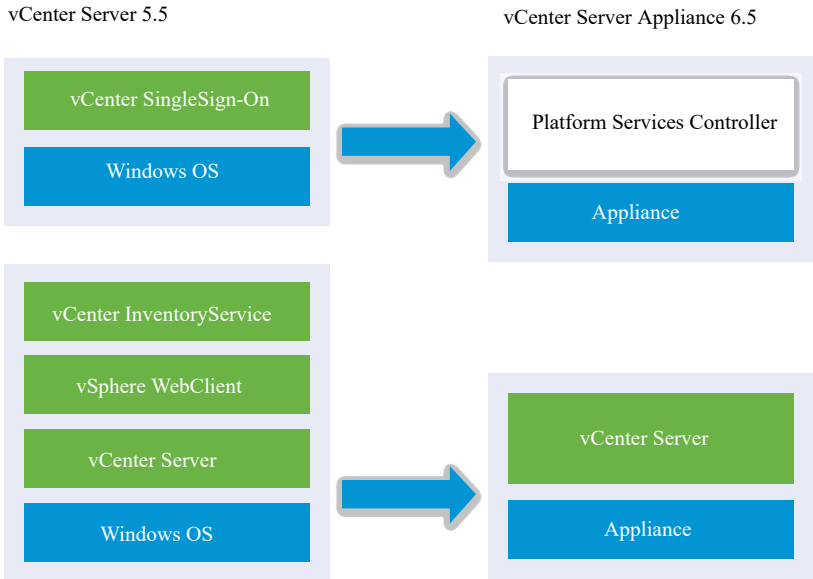
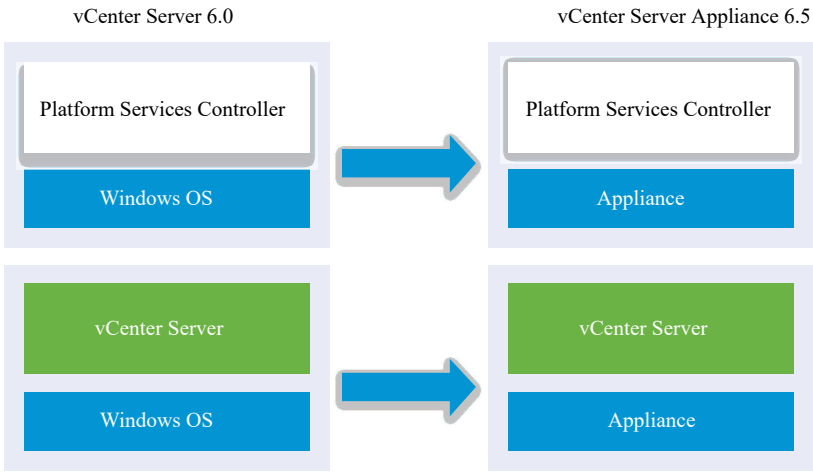


Figure 4-7. vCenter Server 6.0.x with External Platform Services Controller Before and After Migration



When migrating vCenter Server instances on Windows in a mixed platform environment with a Platform Services Controller 6.0 appliance, you upgrade the Platform Services Controller appliance to version 6.5 before migrating the vCenter Server instances to appliances.

When migrating vCenter Server Appliance instances in a mixed platform environment with a Platform Services Controller instance on Windows, you migrate the Platform Services Controller to an appliance before upgrading the vCenter Server Appliance instances to version 6.5.

Important Concurrent migrations of vCenter Single Sign-On or Platform Services Controller instances are not supported. You must migrate the instances in a sequence. See Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments for more details.

GUI tasks for migrating an external vCenter Single Sign-On instance or Platform Services Controller instance from Windows to an appliance:

1 Download and Mount the vCenter Server Appliance Installer ISO file on a network virtual machine or physical server from which you want to perform the migration.

2 Download and Run VMware Migration Assistant on the Source Windows Machine.

   Note If you are migrating a vCenter Server system that uses an external instance of Update Manager that runs on a separate Windows machine, first run Migration Assistant on the Update Manager machine.

3 Assemble the Required Information for Migrating vCenter Server from Windows to an Appliance for each vCenter Single Sign-On, Platform Services Controller, or vCenter Server instance.

4 Deploy the OVA File for Migrating to a Platform Services Controller Appliance.

5 Set Up the Target Platform Services Controller Appliance

6 Deploy the OVA File for the Target vCenter Server Appliance with an External Platform Services Controller

7 Set Up the Target vCenter Server Appliance

Important The user name that you use to log in to the machine from which you want to run the GUI installer, the path to the vCenter Server Appliance installer, and your values including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

For each node to be migrated, the installer:

- Deploys a new target appliance.
- Exports the required files from the source vCenter Single Sign-On, Platform Services Controller, or vCenter Server instance.
- Copies the required files to the target appliance for migration.
- Runs the migration process on the target appliance as specified in the Summary.
- Imports and updates the files and settings of the source vCenter Single Sign-On, Platform Services Controller, or vCenter Server instance to the new appliance.

Deploy the OVA File for Migrating to a Platform Services Controller Appliance

To start the migration process, you use the GUI installer to deploy the OVA file that is included in the installer ISO file as a Platform Services Controller appliance.

Figure 4-8. vCenter Server 5.5 with External vCenter Single Sign-On Before and After Migration

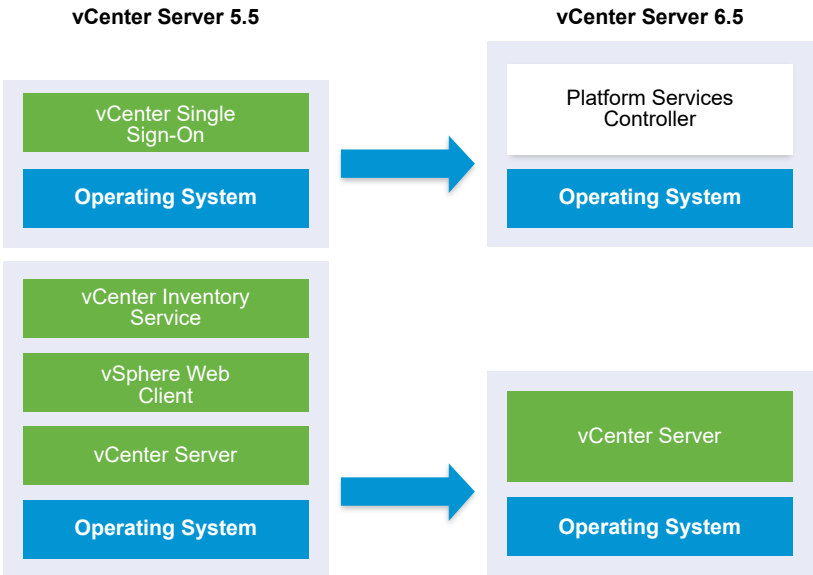
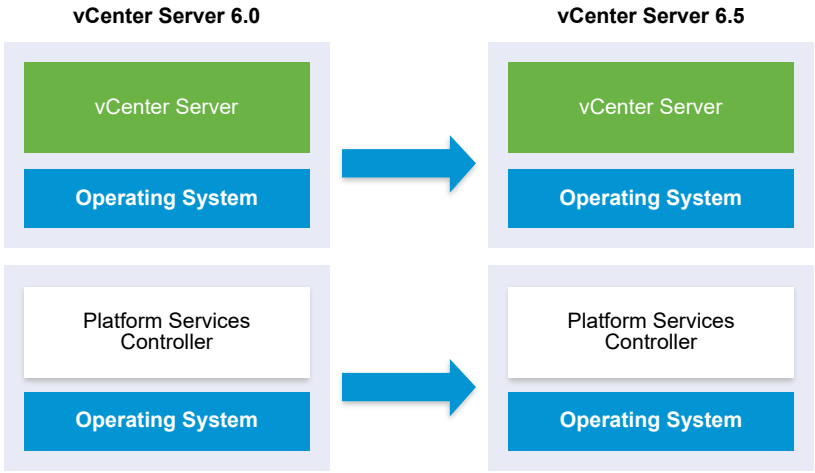


Figure 4-9. vCenter Server 6.0.x with External Platform Services Controller Before and After Migration



Prerequisites

- See Prerequisites for Migrating vCenter Server and Platform Services Controller

Procedure

1. In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Migrate**.
3. Review the Introduction page to understand the migration process and click **Next**.
4. Read and accept the license agreement, and click **Next**.

5 Connect to the target server to which you want to migrate the source vCenter Server.

Option	Steps
You can connect to an ESXi host on which to deploy the target appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the target appliance.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

6 (Optional) Review the warning message and try to resolve the warnings, if any, and click **Yes**.

7 On the Set up target appliance VM page, enter a name for the new Platform Services Controller appliance, set the password for the root user, and click **Next**.

The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

Important The local operating system password is not migrated to the target appliance.

8 On the Connect to source page, enter the details of the vCenter Single Sign-On instance or Platform Services Controller instance and click **Next**.

a Enter the IP address or FQDN.

b Enter the user name and password of a user who has administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user.

c Enter the Migration Assistant Port you received in the Migration Assistant instructions.

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

10 On the Select deployment type page, select **Platform Services Controller** and click **Next**.

11 From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.

12 Configure the temporary network for communication between the Platform Services Controller appliance that you want to upgrade and the new Platform Services Controller appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

13 On the Ready to complete stage 1 page, review the deployment settings for the target Platform Services Controller appliance and click **Finish** to start the OVA deployment process.

14 Wait for the OVA deployment process to complete and click **Continue** to proceed with stage 2 of the migration process to transfer the data from the source vCenter Single Sign-On or Platform Services Controller and set up the services of the new appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the appliance management interface of the newly deployed Platform Services Controller appliance to transfer the data from the source vCenter Single Sign-On instance or Platform Services Controller instance and set up the services.

Results

The newly deployed Platform Services Controller appliance 6.5 is running on the target server but is not configured.

Important The data from the source vCenter Single Sign-On instance or Platform Services Controller instance is not yet transferred and the services of the new appliance are not started.

Set Up the Target Platform Services Controller Appliance

When the OVA deployment completes, you are redirected to stage 2 of the migration process to transfer data from the source vCenter Single Sign-On or Platform Services Controller on Windows to the target appliance and start the services.

Your window of downtime does not begin until you begin to set up the target appliance. You cannot cancel or interrupt the process until it completes with the shutdown of the source deployment. Your window of downtime ends when the target appliance starts.

Procedure

1. Review the introduction to stage 2 of the migration process and click **Next**.
2. On the Select source vCenter Server page, enter the vCenter Single Sign-On administrator password and the root password of the source vCenter Server, enter the password of the user with administrative privileges on the vCenter Server instance, and click **Next**.
3. (Optional) Accept the warning message, if any, by clicking **Yes**.
4. If your source Windows machine is connected to an Active Directory domain, enter the credentials for an administrator domain user with permission to add the target machine to the Active Directory domain, and click **Next**.

   Note The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.

5. 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*.

6. On the Ready to complete page, review the settings for the Platform Services Controller appliance, accept the backup acknowledgement, and click **Finish**.
7. Click **OK** to confirm the shutdown of the source vCenter Single Sign-On or Platform Services Controller and initialize the target appliance.
8. Wait for the data transfer and setup process to complete and click **OK** to go to the Platform Services Controller Getting Started page.

Results

The source vCenter Single Sign-On instance or Platform Services Controller instance is migrated from Windows to a target appliance. The source vCenter Single Sign-On instance or Platform Services Controller instance is powered off and the new target appliance starts.

What to do next

Verify that your Platform Services Controller instance has migrated successfully. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For the new Platform Services Controller appliance to replicate infrastructure data with other Platform Services Controller instances, you must migrate or upgrade all joined Platform Services Controller instances within the vCenter Single Sign-On domain to the same version. For information on upgrading Platform Services Controller instances on Windows, see Upgrade vCenter Single Sign-On 5.5 on Windows or Upgrade vCenter Platform Services Controller 6.0 on Windows.

After you migrate or upgrade all joined Platform Services Controller instances, you can migrate or upgrade the vCenter Server instances within the vCenter Single Sign-On domain. For information on migrating vCenter Server instances to appliances, see Deploy the OVA File for the Target vCenter Server Appliance with an External Platform Services Controller. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 5.5 on Windows or Upgrade vCenter Server 6.0 on Windows.

Deploy the OVA File for the Target vCenter Server Appliance with an External Platform Services Controller

To start the migration process, you use the GUI installer to deploy the OVA file that is included in the installer ISO file as the target vCenter Server Appliance with an external Platform Services Controller

Figure 4-10. vCenter Server 5.5 with External vCenter Single Sign-On Before and After Migration

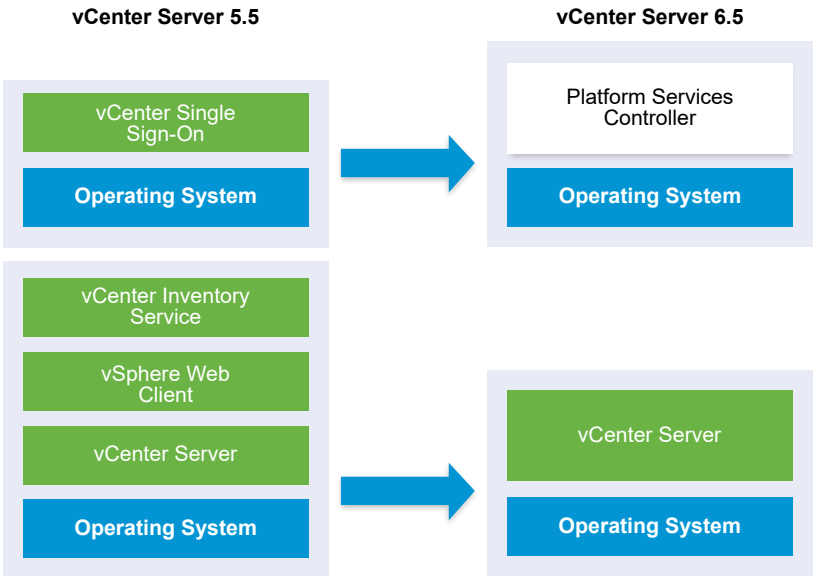
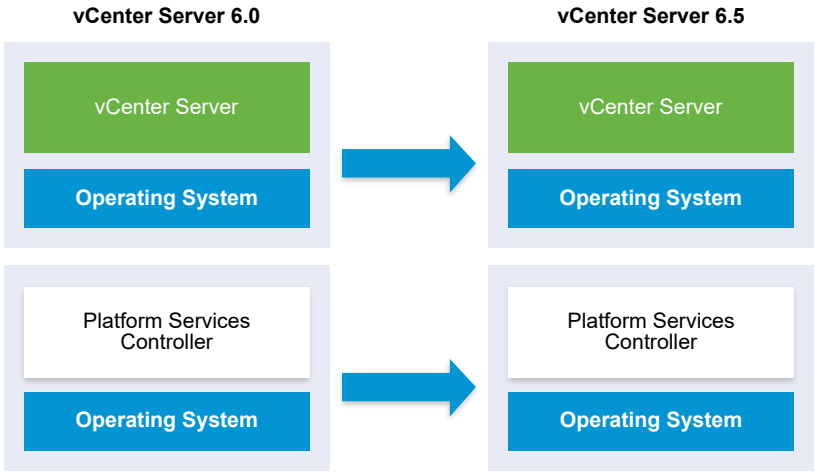


Figure 4-11. vCenter Server 6.0.x with External Platform Services Controller Before and After Migration



Prerequisites

- See Prerequisites for Migrating vCenter Server and Platform Services Controller

Procedure

1. In the vCenter Server Appliance installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Migrate**.
3. Review the Introduction page to understand the migration process and click **Next**.
4. Read and accept the license agreement, and click **Next**.

5 Connect to the target server to which you want to migrate the source vCenter Server.

Option	Steps
You can connect to an ESXi host on which to deploy the target appliance.	1 Enter the FQDN or IP address of the ESXi host. 2 Enter the HTTPS port of the ESXi host. 3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the target appliance.	1 Enter the FQDN or IP address of the vCenter Server instance. 2 Enter the HTTPS port of the vCenter Server instance. 3 Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Accept the certificate warning, if any, by clicking **Yes**. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7 Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

6 (Optional) Review the warning message and try to resolve the warnings, if any, and click **Yes**.

7 On the Set up target appliance VM page, enter a name for the target vCenter Server Appliance, set the password for the root user, and click **Next**.

The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sigh (@), or brackets (()).

Important The local operating system password is not migrated to the target appliance.

8 On the Connect to source page, enter the details for the source vCenter Server instance, and click **Next**.

a Enter the IP address or FQDN.

b Enter the user name and password of a user who has administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user.

c Enter the Migration Assistant Port you received in the Migration Assistant instructions.

9 On the Connect to source instance page, enter the details for the source Windows installation that you want to migrate.

Option	Action
vCenter Server IP Address/FQDN	Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade.
vCenter Single Sign-On administrator user name	Enter the vCenter Single Sign-On administrator user name. If you are upgrading vCenter Server Appliance 5.5.x, this is administrator@vsphere.local.
vCenter Single Sign-On administrator password	Enter the password of the vCenter Single Sign-On administrator.
vCenter Server HTTPS Port	Optionally, change the default vCenter Server HTTPS port number. The default value is 443.

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

11 Select the deployment size for the new vCenter Server Appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 CPUs and 10 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 16 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 24 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 32 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 48 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines

Note At the bottom of the deployment size table, a row shows the size information of the source machine. This size information is reported by the migration assistant and might help understand why you cannot select some deployment sizes.

12 Select the storage size for the new vCenter Server Appliance, and click **Next**.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 250 GB of storage.	Deploys an appliance with 290 GB of storage.	Deploys an appliance with 425 GB of storage.	Deploys an appliance with 640 GB of storage.	Deploys an appliance with 980 GB of storage.
Large	Deploys an appliance with 775 GB of storage.	Deploys an appliance with 820 GB of storage.	Deploys an appliance with 925 GB of storage.	Deploys an appliance with 990 GB of storage.	Deploys an appliance with 1030 GB of storage.
X-Large	Deploys an appliance with 1650 GB of storage.	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1805 GB of storage.	Deploys an appliance with 1870 GB of storage.	Deploys an appliance with 1910 GB of storage.

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 Configure the temporary network for communication between the source vCenter Server and the target vCenter Server Appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. ■ **Static** The wizard prompts you to enter the temporary IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment.

15 On the Ready to complete stage 1 page, review the deployment settings for the target vCenter Server Appliance and click **Finish** to start the OVA deployment process.

16 Wait for the OVA deployment to finish, and click **Continue** to proceed with stage 2 of the deployment process to set up and start the services of the newly deployed appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Appliance Management Interface to set up and start the services.

Results

The newly deployed target vCenter Server Appliance 6.5 with an external Platform Services Controller is running on the target server but is not configured.

Important The data from the source vCenter Server is not yet transferred and the services of the target appliance are not started.

Set Up the Target vCenter Server Appliance

When the OVA deployment completes, you are redirected to stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the newly deployed target vCenter Server Appliance with an external Platform Services Controller.

Your window of downtime does not begin until you begin to set up the target appliance. You cannot cancel or interrupt the process until it completes with the shutdown of the source deployment. Your window of downtime ends when the target appliance starts.

Procedure

1. Review the introduction to stage 2 of the migration process and click **Next**.
2. On the Select source vCenter Server page, enter the vCenter Single Sign-On administrator password and the root password of the source vCenter Server, enter the password of the user with administrative privileges on the vCenter Server instance, and click **Next**.
3. (Optional) Accept the warning message, if any, by clicking **Yes**.
4. If your source Windows machine is connected to an Active Directory domain, enter the credentials for an administrator domain user with permission to add the target machine to the Active Directory domain, and click **Next**.

   Note The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
5. On the Select migration data page, choose the types of data that you want to transfer from the source vCenter Server to the target appliance.

   The large amount of data requires more time to be transferred to the new appliance.
6. On the ready to complete page, review the migration settings, accept the backup acknowledgment, and click **Finish**.
7. Click **OK** to confirm the shutdown of the source vCenter Server.
8. Wait for the data transfer and setup process to finish. Click **OK** to go to the vCenter Server Getting Started page.

Results

The vCenter Server is migrated from Windows to a newly deployed target appliance. The source vCenter Server is powered off and the target appliance starts.

What to do next

Verify that your vCenter Server instances have migrated successfully. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

Complete the migration or upgrade of other vCenter Server instances in the configuration as needed. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 5.5 on Windows or Upgrade vCenter Server 6.0 on Windows.

For post-migration steps, see Chapter 5 After Upgrading or Migrating vCenter Server.

CLI Migration of a vCenter Server Installation from Windows to an Appliance

You can use the CLI installer to automatically migrate a vCenter Server, vCenter Single Sign-On or Platform Services Controller from Windows to an appliance.

The installer ISO file contains example templates of JSON files that contain the minimum configuration parameters required for migrating a vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance from Windows to an appliance. The example templates are located in the `vcsa-cli-installer/templates/migrate` directory.

CLI tasks for migrating your vCenter Server installation from Windows to an appliance:

1 Download and Mount the vCenter Server Appliance Installer.

2 Download and Run VMware Migration Assistant on the Source Windows Machine.

3 Prepare JSON Configuration Files for CLI Migration.

4 Run a Pre-Check Before a CLI Migration to vCenter Server Appliance.

5 Perform a CLI Migration of vCenter Server from Windows to an Appliance.

You can run the CLI installer multiple times with different JSON files to perform multiple CLI migrations, however you cannot run the CLI migrations concurrently.

Important The user name that you use to log in to the machine from which you want to run the CLI installer, the path to the vCenter Server Appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Prepare JSON Configuration Files for CLI Migration

When you use the CLI process to migrate a source vCenter Server installation to a target vCenter Server Appliance, you must prepare a JSON template with the configuration values for the new appliance.

You can migrate vCenter Server, vCenter Single Sign-On, or Platform Services Controller instances from Windows to an appliance by setting values to the configuration parameters in the templates that are available in the installer ISO file. The configuration parameters that are not included in the templates are set to their default values. You can add configuration parameters in the templates to set their values for your migration specification.

The `vcsa-cli-installer/templates/migrate` directory contains example migration templates for CLI migration of vCenter Server 5.5 and vCenter Server 6.0 to an appliance.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run the `vcsa-deploy migrate --template-help` command.

Important The user name that you use to log in to the machine from which you want to run the CLI installer, the path to the vCenter Server Appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Local OS user names for vCenter Server 5.5 are not migrated to the target vCenter Server Appliance and must be recreated after migration is complete. If any local OS user names are used to log in to the vCenter Single Sign-On, you must recreate them in the Platform Services Controller appliance.

Prerequisites

Verify your environment meets the requirements for migration. See System Requirements for Migrating vCenter Server Deployments to vCenter Server Appliance Deployments,

Prepare your environment for migration. See Preparing for Migration.

Procedure

1. Open the `migrate` subfolder in the `vcsa-cli-installer/templates` directory.
2. Copy the migration template from the `migrate` subfolder to your workspace.
   - For vCenter Server 5.5, use the `migrate/winvc5.5/` folder.
   - For vCenter Server 6.0, use the `migrate/winvc6.0/` folder.
3. Open the template file for your use case in a text editor.

   To ensure the correct syntax of your JSON configuration file, use a JSON editor.

4 Fill in values for the required configuration parameters and, optionally, enter additional parameters and their values.

Important To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"C:\\vmware\\vcsa"` sets the path `C:\vmware\vcsa`.

The boolean values must contain only lowercase characters. Can be either `true` or `false`. For example, `"ssh.enable":false`

5 Save in UTF-8 format and close the file.

Results

Your file is ready to use for migration.

What to do next

You can create and save as many templates as are needed for your specific environment. When your template is ready, run the pre-check before using it to run the migration. See Run a Pre-Check Before a CLI Migration to vCenter Server Appliance.

Migration Configuration Parameters

When using the CLI installer to migrate your vCenter Server installation to an appliance, you must provide the parameters with values for your migration specification.

The table lists the configuration parameters that you use to provide input data for the source vCenter Server.

Important The path to the vCenter Server Appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"C:\\vmware\\vcsa"` sets the path `C:\vmware\vcsa`.

The boolean values must contain only lowercase characters. Can be either `true` or `false`. For example, `"ssh.enable":false`.

Sections and Subsections of Configuration Parameters in the JSON Migration Templates

The configuration parameters in the JSON migration templates are organized in sections and subsections.

Table 4-5. Sections and Subsections of Configuration Parameters in the JSON Migration Templates

Section	Subsection	Description
`new.vcsa` - describes the target appliance that you want to migrate to	`esxi`	Use only if you want to deploy the appliance directly on an ESXi host. Contains the configuration parameters that describe the target ESXi host. **Note** You must fill in either the `esxi` or the `vc` subsection.
	`vc`	Use only if you want to deploy the appliance on the inventory of a vCenter Server instance. Contains the configuration parameters that describe the target ESXi host or DRS cluster from the vCenter Server inventory. **Note** You must fill in either the `vc` or the `esxi` subsection.
	`appliance`	Contains the configuration parameters that describe the appliance.
	`os`	Contains the configuration parameters that describe the operating system settings for the appliance.
	`ovftool.arguments`	Optional subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates. **Important** The vCenter Server Appliance installer does not validate the configuration parameters in the `ovftool.arguments` subsection. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
	`temporary.network`	Contains the configuration parameters that describe the temporary network for migrating the data from the source to the new target appliance.
	`user-options`	Use only when the source is a vCenter Server instance. Contains the configuration parameters that let you control aspects of the migration process for particular components.
`source.vc` - describes the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller	`vc.win`	Contains the configuration parameters that describe the source Windows installation of vCenter Server, vCenter Single Sign-On, or Platform Services Controller

Table 4-5. Sections and Subsections of Configuration Parameters in the JSON Migration Templates (continued)

Section	Subsection	Description
	`run.migration.assistant`	Use only if the source Windows installation is running as a virtual machine and you want to automate the invocation of Migration Assistant. For a source Windows installation running on a physical machine, or if you are running Migration Assistant manually on the source Windows machine, copy and paste the thumbprint value from the Migration Assistant console output on the source machine to the `migration.ssl.thumbprint` key in the `vc.win` subsection, and remove the `run.migration.assistant` section.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP)	`settings`	Contains only the `ceip.enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). Required only if you are deploying a vCenter Server Appliance with an embedded vCenter Single Sign-On or a Platform Services Controller appliance. **Note** If set to `true`, you must run the CLI deployment command with the `--acknowledge-ceip` argument. For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

Configuration Parameters in the `new.vcsa` Section

Table 4-6. Configuration Parameters in the `new.vcsa` Section, `esxi` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target ESXi host on which you want to deploy the appliance.
`username`	string	A user name with administrative privileges on the target ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the target ESXi host.
`deployment.network`	string	The name of the network to which to connect the appliance. **Note** The network must be accessible from the target ESXi host. Ignored if the target ESXi host has only one network.
`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the appliance. **Note** The datastore must be accessible from the ESXi host. The datastore must have enough free space.
`port`	integer	The port number of the ESXi host. The default port is 443.

Table 4-7. Configuration Parameters in the `new.vcsa` Section, `vc` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target vCenter Server instance on which you want to deploy the appliance.
`username`	string	vCenter Single Sign-On administrator user name on the target vCenter Server instance, for example, administrator@vsphere.local.
`password`	string	The password of the vCenter Single Sign-On administrator user on the target vCenter Server instance.
`deployment.network`	string	The name of the network to which to connect the appliance. **Note** The network must be accessible from the target ESXi host or DRS cluster on which you want to deploy the appliance. Ignored if the target ESXi host or DRS cluster has only one network.

`datacenter`	string or array	The vCenter Server datacenter that contains the target ESXi host or DRS cluster on which you want to deploy the appliance.
		If the datacenter is located in a folder or a structure of folders, the value must be either a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "datacenter_name"]`
		or
		`"parent_folder, child_folder, datacenter_name"`
		Note The value is case-sensitive.

`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the appliance. **Note** The datastore must be accessible from the target ESXi host or DRS cluster. The datastore must have at least 15 GB of free space.
`port`	integer	The port number of the vCenter Server. The default port is 443.

Table 4-7. Configuration Parameters in the `new.vcsa` Section, `vc` Subsection (continued)

Name	Type	Description

`target`	string or array	The target ESXi host or DRS cluster on which you want to deploy the appliance.
		Important You must provide the name that is displayed in the vCenter Server inventory. For example, if the name of the target ESXi host is an IP address in the vCenter Server inventory, you cannot provide an FQDN.
		If the target ESXi host or DRS cluster is located in a folder or a structure of folders, the value must be a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		or
		`"parent_folder, child_folder, esxi-host.domain.com"`
		If the target ESXi host is part of a cluster, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["cluster_name", "esxi-host.domain.com"]`
		or
		`"cluster_name, esxi-host.domain.com"`
		Note The value is case-sensitive.

`vm.folder`	string	Optional. The name of the VM folder to which to add the appliance.

Table 4-8. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection

Name	Type	Description
`thin.disk.mode`	Boolean	Set to `true` to deploy the appliance with thin virtual disks.
`deployment.option`	string	The size of the appliance. ■ Set to `tiny` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 8 GB of memory, and 250 GB of storage. ■ Set to `tiny-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 8 GB of memory, and 775 GB of storage. ■ Set to `tiny-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 8 GB of memory, and 1650 GB of storage. ■ Set to `small` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 290 GB of storage. ■ Set to `small-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 820 GB of storage. ■ Set to `small-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1700 GB of storage. ■ Set to `medium` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 425 GB of storage. ■ Set to `medium-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 925 GB of storage. ■ Set to `medium-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the x-large storage size.

Table 4-8. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 8 CPUs, 24 GB of memory, and 1805 GB of storage. ■ Set to `large` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 640 GB of storage. ■ Set to `large-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 990 GB of storage. ■ Set to `large-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1870 GB of storage. ■ Set to `xlarge` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 980 GB of storage. ■ Set to `xlarge-lstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 1030 GB of storage. ■ Set to `xlarge-xlstorage` if you want to deploy a vCenter Server Appliance with an embedded Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 1910 GB of storage. ■ Set to `management-tiny` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 8 GB of memory, and 250 GB of storage. ■ Set to `management-tiny-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 8 GB of memory, and 775 GB of storage. ■ Set to `management-tiny-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the x-large storage size.

Table 4-8. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 2 CPUs, 8 GB of memory, and 1650 GB of storage. ■ Set to `management-small` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 290 GB of storage. ■ Set to `management-small-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 820 GB of storage. ■ Set to `management-small-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1700 GB of storage. ■ Set to `management-medium` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 425 GB of storage. ■ Set to `management-medium-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 925 GB of storage. ■ Set to `management-medium-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1805 GB of storage. ■ Set to `management-large` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 640 GB of storage. ■ Set to `management-large-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 990 GB of storage. ■ Set to `management-large-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size.

Table 4-8. Configuration Parameters in the `new.vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 16 CPUs, 32 GB of memory, and 1870 GB of storage. ■ Set to `management-xlarge` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 980 GB of storage. ■ Set to `management-xlarge-lstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 1030 GB of storage. ■ Set to `management-xlarge-xlstorage` if you want to deploy a vCenter Server Appliance with an external Platform Services Controller for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 48 CPUs, 24 GB of memory, and 1910 GB of storage. ■ Set to `infrastructure`if you want to deploy a Platform Services Controller appliance. Deploys an appliance with 2 CPUs, 4 GB of memory, and 60 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server Appliance installation package. By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool.path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 4-9. Configuration Parameters in the `new.vcsa` Section, `os` Subsection

Name	Type	Description
`password`	string	The password for the root user of the appliance operating system. The password must contain between 8 and 20 characters, at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!). All characters must be lower ASCII characters without spaces.
`ssh.enable`	Boolean	Set to `true` to enable SSH administrator login to the appliance.

Table 4-10. Configuration Parameters in the `new.vcsa` Section, `temporary.network` Subsection

Name	Type	Description
`ip.family`	string	IP version for the network of the appliance. Set to `ipv4` or `ipv6`.
`mode`	string	IP assignment for the network of the appliance. Set to `static` or `dhcp`.
`ip`	string	IP address for the appliance. Required only if you use static assignment, that is, if you set the `mode` parameter to `static`. You must set an IPv4 or IPv6 address that corresponds to the network IP version, that is, to the value of the `ip.family` parameter. An IPv4 address must comply with the RFC 790 guidelines. An IPv6 address must comply with the RFC 2373 guidelines.

`dns.servers`	string or array	IP addresses of one or more DNS servers.
		To set more than one DNS server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`
		Required only if you use static assignment, that is, if you set the `mode` parameter to `static`.

`prefix`	string	Network prefix length. Required only if you use assignment, that is, if you set the `mode` parameter to `static`. For IPv4 version, the value must be between `0` and `32`. For IPv6 version, the value must be between `0` and `128`.
`gateway`	string	IP address of the default gateway. For IPv6 version, the value can be `default`.
`system.name`	string	Primary network identity. Can be an IP address or FQDN, preferably FQDN. You cannot change the value of this parameter after the deployment. The FQDN and dotted-decimal numbers must comply with the RFC 1123 guidelines.

Table 4-11. Configuration Parameters in the `new.vcsa` Section, `user-options` Subsection

Name	Type	Description
`vcdb.migrateSet`	string	Set data migration option. Available options are `core`, `all`, and `core_events_tasks`. Set to `core` to migrate core inventory and configuration data. Set to `all`to migrate all vCenter Server performance and historical data such as stats, events, alarms, and tasks. Not migrating all data reduces the amount of overall downtime.

Requirements for the Automatic Invocation of Migration Assistant

You use the `run.migration.assistant` subsection to automate the invocation of Migration Assistant. Automatic invocation works only if the source Windows installation is running as a virtual machine.

The user account that you specify in the `os.username` or `vum.os.username` parameters must not need privilege elevation to Administrator. For example:

- The built-in Windows Administrator account
- A user account with a user name other than Administrator that is a member of the local Windows Administrators group
- The Domain Administrator account with the user name Administrator that is a member of the local Windows Administrators group
- The user name ID must be in the format *your_domain_name**user_ID*. Do not use the format *user_ID@your_domain_name*.

Restriction Automatic invocation of Migration Assistant does not work with a Windows account that requires privilege elevation to Administrator. Instead, run Migration Assistant manually on the source Windows machine, copy and paste the thumbprint value from the Migration Assistant console output on the source machine to the `migration.ssl.thumbprint` key in the `vc.win` subsection, and remove the `run.migration.assistant` section.

Configuration Parameters in the `source.vc` Section

Table 4-12. Configuration Parameters in the `source.vc` Section, `vc.win` Subsection

Name	Type	Description
`hostname`	string	The host name or IP address of the source Windows installation of vCenter Server, vCenter Single Sign-On, or Platform Services Controller that you want to migrate.
`username`	string	A vCenter Single Sign-On user name with administrative privileges for the vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance that you want to migrate.
`password`	string	The password of the vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance that you want to migrate.
`migration.port`	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
`active.directory.domain`	string	The name of the Active Directory domain to which the source vCenter Server instance is joined.
`active.directory.username`	string	Administrator user name of the Active Directory domain to which the source vCenter Server instance is joined.

Table 4-12. Configuration Parameters in the `source.vc` Section, `vc.win` Subsection (continued)

Name	Type	Description
`active.directory.password`	string	Administrator password of the Active Directory domain to which the source vCenter Server instance is joined. **Note** The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
`migration.ssl.thumbprint`	string	The SSL thumbprint of Migration Assistant.

Table 4-13. Configuration Parameters in the `source.vc` Section, `run.migration.assistant` Subsection

Name	Type	Description
`esxi.hostname`	string	FQDN or IP address of ESXi on which the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance resides.
`esxi.username`	string	User name of a user with administrative privileges on the ESXi host.
`esxi.password`	string	The password of the ESXi host user. If left blank, or omitted, you will be prompted to enter the password at the command console during template verification.
`esxi.port`	string	The port number of the ESXi host. The default port is 443.
`os.username`	string	Administrator user name for the source Windows machine.
`os.password`	string	Administrator user password for the source Windows machine. If left blank, or omitted, you will be prompted to enter it at the command console during template verification.
`migration.ip`	string	The IP address of the network adapter that will be migrated.
`migration.port`	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
`export.dir`	string	Directory to export source configuration and data.
`sa.password`	string	The IP address of the network vCenter Server service account user password. This option is only required if the vCenter Server service is running under a non LocalSystem account. If left blank, or omitted, you will be prompted to enter it at the command console during template verification.

Table 4-14. Configuration Parameters in the `source.vum` Section, `run.migration.assistant` Subsection

Name	Type	Description
`esxi.hostname`	string	FQDN or IP address of ESXi on which the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance resides.
`esxi.username`	string	User name of a user with administrative privileges on the ESXi host.

Table 4-14. Configuration Parameters in the `source.vum` Section, `run.migration.assistant` Subsection (continued)

Name	Type	Description
`esxi.password`	string	The password of the ESXi host user. If left blank, or omitted, you will be prompted to enter the password at the command console during template verification.
`esxi.port`	string	The port number of the ESXi host. The default port is 443.
`vum.hostname`	string	FQDN or IP address of ESXi on which the source Update Manager instance resides.
`vum.os.username`	string	Administrator user name for the source Windows machine.
`vum.os.password`	string	Administrator user password for the source Update Manager Windows machine. If left blank, or omitted, you will be prompted to enter it at the command console during template verification.
`migration.port`	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
`export.dir`	string	Directory to export source configuration and data.

Configuration Parameters in the `ceip` Section

Table 4-15. Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
`ceip.enabled`	Boolean	Set to `true` to join the CEIP for this appliance.

Run a Pre-Check Before a CLI Migration to vCenter Server Appliance

You can run a pre-check to verify that the migration requirements are met and resolve any problems before migration of your vCenter Server deployment.

Before migrating your vCenter Server deployment to an appliance, you can run a pre-check to find out the disk space requirement, the estimated upgrade time, and the extensions registered with vCenter Server Appliance. Running pre-upgrade is an optional but highly recommended step when planning your upgrade.

Prerequisites

Prepare JSON Configuration Files for CLI Migration using the example templates and Migration Configuration Parameters.

Procedure

1 Run `CLI Migrate` using the `--pre-check-only` option.

   You can adjust your migration plans using the disk space requirements and estimated migration time. If you receive an error, you can troubleshoot and resolve the problem before the actual migration.

2 Verify your template without deploying the appliance by entering the command: `vcsa-deploy migrate --verify-only` *`path_to_json_file`*.

3 After resolving any errors, run the `CLI Migrate` command using the `--verify-only` option again until all errors are resolved.

Results

You are now prepared for an error-free CLI migration process.

What to do next

Perform a CLI Migration of vCenter Server from Windows to an Appliance.

Perform a CLI Migration of vCenter Server from Windows to an Appliance

You can migrate vCenter Server to an appliance from a machine that is in your vSphere network.

Prerequisites

- See Prerequisites for Migrating vCenter Server and Platform Services Controller
- Create a snapshot of the deployment that you want to migrate as a precaution in case of failure during the migration process.
- Download the installer ISO file from the VMware website to a machine that is in your vSphere network. The installer ISO filename is VMware-VCSA-all-6.5.0-yyyyyy.iso, where yyyyyy is the build number. See Download and Mount the vCenter Server Appliance Installer.
- Prepare JSON Configuration Files for CLI Migration.
- Run a Pre-Check Before a CLI Migration to vCenter Server Appliance to identify problems and refine your migration plan.
- Review the optional arguments for running the migration. See Syntax of the CLI Migrate Command.

Procedure

1 Navigate to the software CLI installer directory for your operating system.
   - If you are deploying the appliance from a machine with Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are deploying the appliance from a machine with Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are deploying the appliance from a machine with Mac OS, navigate to the `vcsa-cli-installer/mac` directory.

2 Select the CLI installer: vcsa-deploy.exe.

3 Run the migration command.

```
vcsa-deploy migrate --accept-eula optional_arguments path_to_the_json_file
```

The *optional_arguments* variable is a space-separated list of optional arguments to set additional configurations.

For example, you can set the location of the log and other output files that the installer generates.

```
vcsa-deploy migrate --accept-eula --log-dir=path_to_the_location path_to_the_json_file
```

Results

The migration template is deployed. You can Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

Syntax of the CLI Migrate Command

You can use one or more command arguments to set the execution parameters of the migrate command.

You can add a space-separated list of arguments to the CLI upgrade command.

```
vcsa-deploy migrate list_of_arguments path_to_the_json_file
```

The required `template` argument provides the path of a JSON file that describes the vCenter Server Appliance deployment procedure.

Important The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"C:\\vmware\\vcsa"` sets the path `C:\vmware\vcsa`.

The boolean values must contain only lowercase characters. Can be either `true` or `false`. For example, `"ssh.enable":false`.

Optional Argument	Description
`--accept-eula`	Accepts the end-user license agreement. Required for executing the deployment command.
`-h, --help`	Displays the help message for the command.
`--template-help`	Displays the help message for the configuration parameters in the JSON deployment file. You can use `vcsa-deploy [subcommand] --help` for a list of subcommand-specific arguments.
`-v, --verbose`	Adds debug information to the console output.

Optional Argument	Description
`-t`, `--terse`	Hides the console output. Displays only warning and error messages.
`--log-dir`, `LOG_DIR`	Sets the location of the log and other output files that the installer generates.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters in the JSON file and deploys the appliance. Does not perform verification of the OVF Tool parameters.
`--no-esx-ssl-verify`	Skips the SSL verification for ESXi connections. **Important** Avoid using this option because it might cause problems during deployment or after deployment because of invalidated values passed to the appliance.
`deployment-target-ssl-thumbprint TARGET_THUMBPRINT`	Sets the thumbprint to pass to the OVF Tool for verifying the ESXi or vCenter Server deployment target.
`--verify-only`	Performs basic verification of the configuration parameters in the JSON file and verification of the OVF Tool parameters. Does not deploy the appliance.
`--verify-template-only`	Performs the basic template verification without installing Upgrade Runner, running prechecks, or upgrading the vCenter Server Appliance.
`--precheck-only`	Installs Migration Assistant on the source vCenter Server virtual machine instance and runs a complete set of prechecks without performing the migration.
`--acknowledge-ceip`	Confirms acknowledgement of your VMware Customer Experience Improvement Program (CEIP) participation. This argument is required if **`ceip.enabled`** is set to true in the upgrade template.

Exit Code	Description
0	Command ran successfully
1	Runtime error
2	Validation error
3	Template error

After Upgrading or Migrating vCenter Server

5

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.
- If you migrated vCenter Server on Windows to a target vCenter Server Appliance and you use any local OS user names to log in to the vCenter Single Sign-On, you must recreate them and reassign permissions in the Platform Services Controller appliance.
- If you performed an upgrade, upgrade any additional modules that are linked to this instance of vCenter Server, such as Update Manager. If you performed a migration from vCenter Server on Windows to a vCenter Server Appliance, the Update Manager module is migrated as well.
- Optionally, upgrade or migrate the ESXi hosts in the vCenter Server inventory to the same version as the vCenter Server instance.
- If you use Update Manager in your vCenter Server deployment, and Update Manager and vCenter Server were running on separate machines prior the migration, consider to shut down or delete the Update Manager host machine after the migration is complete. Before disposing of the Update Manager host machine, take into account the following:
  - You might need the host machine for rolling back purposes of your upgraded or migrated environment.
  - You might have other software that runs on that machine.

This chapter includes the following topics:

- Roll Back a vCenter Server Appliance Upgrade or vCenter Server on Windows Migration

Verify Your vCenter Server Appliance Upgrade or Migration Is Successful

You can verify the success of your vCenter Server Appliance upgrade or migration.

You must be logged into the upgraded or migrated vCenter Server instance. If you created a reference of required information based or a CLI template, you can use it to validate the upgrade or migration success.

Procedure

1. Verify that the IP address is correct.
2. Verify that the Active Directory registration has not changed.
3. Verify the Network registration is correct.
4. Verify the Domain is correct.
5. Verify the certificates are valid.
6. Verify the inventory data is correctly migrated.
   a. Review the events history.
   b. Review the performance charts.
   c. Review the users, permissions, and roles.

Results

If the postupgrade or postmigration configuration conforms to your required information or CLI template reference and expectations, the vCenter Server upgrade or migration is complete.

What to do next

You can troubleshoot unexpected behavior by reviewing logs. You can also perform a rollback to the source configuration. See Roll Back a vCenter Server Appliance Upgrade or vCenter Server on Windows Migration

Log in to vCenter Server by Using the vSphere Web Client

Log in to vCenter Server by using the vSphere Web Client to manage your vSphere inventory.

In vSphere 6.0 and later, the vSphere Web Client is installed as part of the vCenter Server on Windows or the vCenter Server Appliance deployment. This way, the vSphere Web Client always points to the same vCenter Single Sign-On instance.

Procedure

1 Open a Web browser and enter the URL for the vSphere Web Client: **`https://`** ***`vcenter_server_ip_address_or_fqdn`*****`/vsphere-client`**.

2 Enter the credentials of a user who has permissions on vCenter Server, and click **Login**.

3 If a warning message about an untrusted SSL certificate appears, select the appropriate action based on your security policy.

Option	Action
Ignore the security warning for this login session only.	Click **Ignore**.
Ignore the security warning for this login session, and install the default certificate so that the warning does not appear again.	Select **Install this certificate and do not display any security warnings for this server** and click **Ignore**. Select this option only if using the default certificate does not present a security problem in your environment.
Cancel and install a signed certificate before proceeding.	Click **Cancel** and ensure that a signed certificate is installed on the vCenter Server system before you attempt to connect again.

Results

The vSphere Web Client connects to all the vCenter Server systems on which the specified user has permissions, allowing you to view and manage your inventory.

Install the VMware Enhanced Authentication Plug-in

The VMware Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality.

In this vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaces the Client Integration Plug-in from vSphere 6.0 releases and earlier. The Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality. These are the only two features carried over from the previous Client Integration Plug-in. The Enhanced Authentication Plug-in can function seamlessly if you already have the Client Integration Plug-in installed on your system from vSphere 6.0 or earlier. There are no conflicts if both plug-ins are installed.

Watch the video "vSphere Web Client after the Client Integration Plug-in Removal" for more information about the workflow changes to the vSphere Client:

vSphere Web Client after the Client Integration Plug-in Removal (https://vmwaretv.vmware.com/media/t/1_6bib1xjv)

Install the plug-in only once to enable all the functionality the plug-in delivers.

For information about supported browsers and operating systems, see the *vSphere Installation and Setup* documentation.

Procedure

1 Open a Web browser and type the URL for the vSphere Web Client.

2 At the bottom of the vSphere Web Client login page, click **Download Enhanced Authentication Plug-in**.

3 If the browser blocks the installation either by issuing certificate errors or by running a pop-up blocker, follow the Help instructions for your browser to resolve the problem.

4 Save the plug-in to your computer, and run the executable.

5 Step through the installation wizard for both the VMware Enhanced Authentication Plug-in and the VMware Plug-in Service which are run in succession.

6 When the installations are complete, refresh your browser.

7 On the External Protocol Request dialog box, click **Launch Application** to run the Enhanced Authentication Plug-in.

   The link to download the plug-in disappears from the login page.

Collect vCenter Server Log Files

After you install vCenter Server, you can collect the vCenter Server log files for diagnosing and troubleshooting purposes.

Note This procedure provides information about how to collect the log files for a Windows installation of vCenter Server. For information about exporting a support bundle and browsing the log files in the vCenter Server Appliance, see *vCenter Server Appliance Configuration*.

Procedure

1 Log in as an administrator on the Windows machine where vCenter Server is installed.

2 Navigate to **Start > Programs > VMware > Generate vCenter Server log bundle** to generate the log bundle.

   You can generate vCenter Server log bundles even if you are unable to connect to the vCenter Server by using the vSphere Web Client

Results

The log files for the vCenter Server system are generated and saved in a `.tgz` archive on your desktop.

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 were always able to 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 is created when you install vCenter Single Sign-On.

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 *Platform Services Controller Administration*.

Reregister Solution in vCenter Server after Upgrade or Migration

You need to reregister a previously registered plug-in package with your vCenter Server when certificate has been regenerated during the upgrade or migration process.

Consult the vendor documentation for any solution-based vCenter Server extensions and client plug-ins for instructions to re-register after a vCenter Server upgrade or migration.

If the procedure provided by your plug-in solution vendor fails to reregister the plug-in, you can use the following procedure to remove the plug-in registration, and then register it again with vCenter Server. For information on registering plug-ins, see the *vCenter Server and Host Management* documentation. For information on removing or disabling unwanted plug-ins from vCenter Server, see Knowledge Base article KB 102536.

Before you can reregister a plugin, you must unregister the solution.

Procedure

1 In a Web browser, navigate to the Managed Object Browser of your vCenter Server.

  `https://vcenter_server_ip_address_or_fqdn/mob/?moid=ExtensionManager`

2 Log in with your vCenter Server credentials.

3 On the `ManagedObjectReference:ExtensionManager` page, under Methods, click **UnregisterExtension**.

4 On the `void UnregisterExtension` page, in the text box inside the Value column, enter the value for the `key` property of the `Extension` data object of your vSphere Web Client extension.

5 Click **Invoke Method** to unregister the extension.

What to do next

Go to the solution registration page and register the plug-in.

Verify that your extension is registered successfully with vCenter Server by using one of the following approaches.

- Log in to the vSphere Web Client. See Log in to vCenter Server by Using the vSphere Web Client.
- In the vSphere Web Client, go to Administration and under Solutions, select **Client Plug-Ins** and click **Check for New Plug-Ins**.
- Log out and log in again to the vSphere Web Client. The vSphere Web Client checks for new plug-ins for each new user session

Roll Back a vCenter Server Appliance Upgrade or vCenter Server on Windows Migration

You can roll back a vCenter Server Appliance upgrade or migration by reverting to the source appliance or vCenter Server on Windows.

The roll back steps apply in the following upgrade and migration contexts:

- vCenter Server Appliance with an embedded Platform Services Controller
- vCenter Server Appliance with an external Platform Services Controller

Prerequisites

You must have access to the source vCenter Server Appliance or vCenter Server on Windows.

Procedure

- To revert a failed migration of vCenter Server, see Knowledge Base article KB 2146453.

Changing a vCenter Server Deployment Type After Upgrade or Migration

6

You can change your vCenter Server deployment type after upgrade or migration to version 6.5.

This chapter includes the following topics:

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.
- If you want to repoint a vCenter Server Appliance that is configured in a vCenter HA cluster, remove the vCenter HA configuration. For information about removing a vCenter HA configuration, see *vSphere Availability*.

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 instance is running and can be managed.

Results

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

What to do next

If you repointed a vCenter Server Appliance that was configured in a vCenter HA cluster, you can reconfigure the vCenter HA cluster. For information about configuring vCenter HA, see *vSphere Availability*.

Patching and Updating vCenter Server 6.5 Deployments

7

You can update the vCenter Server Appliance with patches by using the `software-packages` utility available in the vCenter Server Appliance shell. You can update the Java components and vCenter Server for Windows tc Server with VIMPatch.

This chapter includes the following topics:

- Patching the vCenter Server Appliance and Platform Services Controller Appliance
- Update the Java Components and vCenter Server tc Server with VIMPatch

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 makes patches available on a monthly basis. These patches can only be applied in between major releases of vCenter Server Appliance. For example, patches released for the initial release of vCenter Server Appliance 6.7, are not applicable to vCenter Server Appliance 6.7 Update 1, as any patches previously made available will be included with the Update 1 release.

These patches can be for core product functionality, other packages in the vCenter Server such as Photon, or both.

Note You must use only the patches provided by VMware to update the packages in your vCenter Server. Updating these packages through any other means may impact the product functionality.

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 a single type of ISO image that contains patches.

Download Filename	Description
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 and Photon 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.

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.

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. The custom patching repository runs on a local Web server within your data center and replicates the data from the default repository. Optionally, you can set up an 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. Log in to VMware Customer Connect at https://customerconnect.vmware.com/patch/.
   b. Select VC from the **Select a Product** drop-down and the vCenter Server version from the **Select Version** drop-down.
   c. Click **SEARCH**.
   d. Download the ISO image.
   e. Confirm that the md5sum is correct by using an MD5 checksum tool.
   f. On your Web server, create a repository directory under the root.

      For example, create the **`vc_update_repo`** directory.
   g. 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, `https://web_server_name.your_company.com/vc_update_repo`. The repository URL must use a secure protocol such as HTTPS or FTPS.

5 If the specified repository requires authentication, enter the user name and password.

6 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 patches. You must apply patches to the Platform Services Controller and any replicating partners 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. The custom patching repository runs on a local Web server within your data center and replicates the data from the default repository. Optionally, you can set up an 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 Log in to VMware Customer Connect at https://customerconnect.vmware.com/patch/.

b Select VC from the **Select a Product** drop-down and the vCenter Server version from the **Select Version** drop-down.

c Click **SEARCH**.

d Download the ISO image.

e Confirm that the md5sum is correct by using an MD5 checksum tool.

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

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

g 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 https://web_server_name.your_company.com/vc_update_repo [--
username username] [--password password]
```

where the square brackets [] enclose the command options.

The repository URL must use a secure protocol such as HTTPS or FTPS. 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 patches. You must apply patches to the Platform Services Controller and any replicating partners 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 now -r "patch reboot"
```

Patch a vCenter High Availability Environment

This procedure describes how to patch the Active, Passive, and Witness node if your vCenter Server Appliance is configured in a vCenter High Availability (HA) cluster.

A vCenter High Availability cluster consists of three vCenter Server Appliances that act as an Active, Passive, and Witness node. For information about configuring vCenter High Availability, see *vSphere Availability*.

You patch the three nodes in a sequence and use a manual failover so that you always patch a non-Active node. For patching the nodes, you must use the `software-packages` utility from the appliance shell. For information about patching the appliance from the appliance shell, see Patching the vCenter Server Appliance by Using the Appliance Shell.

Prerequisites

Verify that patching a vCenter HA configuration is supported for your version of vCenter Server Appliance. For certain vCenter Server 6.7 patch releases, you must remove the vCenter HA configuration and update the vCenter Server Appliance using either the vCenter Server Appliance Management Interface or the `software-packages` utility in the appliance shell of a vCenter Server Appliance. To learn if your version of vCenter Server Appliance can be patched using this procedure, see Knowledge Base article KB 55938.

Procedure

1 Place the vCenter HA cluster in maintenance mode.
   a In the vSphere Client inventory, click the **Configure** tab.
   b Under **Settings**, select **vCenter HA** and click **Edit**.
   c Select **Maintenance Mode** and click **OK**.
2 Log in as root to the appliance shell of the Active node by using the public IP address.
3 Patch the Witness node.
   a From the appliance shell of the Active node, access the Bash shell and establish an SSH session to the Witness node.

      ```
      ssh root@Witness_node_IP_address
      ```

   b Patch the Witness node.

      Use the `software-packages` utility.

   c Exit the SSH session to the Witness node.

      ```
      exit
      ```

4 Patch the Passive node.
   a From the appliance shell of the Active node, access the Bash shell and establish an SSH session to the Passive node.

      ```
      ssh root@Passve_node_IP_address
      ```

   b Patch the Passive node.

      Use the `software-packages` utility.

   c Exit the SSH session to the Passive node.

      ```
      exit
      ```

5 Log out from the appliance shell of the Active node.
6 Initiate a vCenter HA failover manually.
   a Log in to the Active node with the vSphere Client and click **Configure**.
   b Under **Settings**, select **vCenter HA** and click **Initiate Failover**.
   c To start the failover click **Yes**.

      A dialog box offers you the option to force a failover without synchronization. In most cases, performing synchronization first is best.

   You can see in the vSphere Client that the Passive node has become the Active node and the Active node has become the Passive node.
7 Log in as root to the appliance shell of the new Active node by using the public IP address.

8 Patch the new Passive node.

   a From the appliance shell of the Active node, access the Bash shell and establish an SSH session to the Passive node.

   ```
   ssh root@Passve_node_IP_address
   ```

   b Patch the Passive node.

   Use the `software-packages` utility.

   c Exit the SSH session to the Passive node.

   ```
   exit
   ```

9 Log out from the appliance shell of the Active node.

10 Exit the maintenance mode.

   a In the vSphere Client inventory, click the **Configure** tab.

   b Under **Settings**, select **vCenter HA** and click **Edit**.

   c Select **Turn On vCenter HA** and click **OK**.

Patch a Platform Services Controller High Availability Environment

This procedure describes how to patch a Platform Services Controller configured in a High Availability (HA) environment.

Platform Services Controller high availability deployments have at least two joined Platform Services Controller instances in a vCenter Single Sign-On domain. The Platform Services Controller instances use a third-party load balancer to ensure automatic failover without downtime in the event an instance becomes unavailable.

Using the load balancer, you must disable monitoring and node membership on the first Platform Services Controller instance (Node 1), and redirect all connecting clients to the second Platform Services Controller (Node 2). You can then patch Node 1. After successfully patching Node 1, redirect all connecting clients to Node 1 and patch Node 2.

Prerequisites

- Verify that a backup of the Platform Services Controller appliances exist.
- Mount the upgrade `.iso` file to the virtual appliances.
- Ensure that you understand how to redirect the network traffic, and both enable and disable health monitoring on the load balancer in use in your environment. For more information, see *vSphere Networking*.

Procedure

1 Log in to vCenter Server using the vSphere Web Client.

2 Direct traffic to Platform Services Controller Node 2, and disable health monitoring on the load balancer.

3 In a Web browser, go to the Platform Services Controller virtual appliance management interface (VAMI) to configure the appliance system settings interface at `platform_services_controller_ip:5480`.

   Log in as root. The default root password is the virtual appliance root password that you set when deploying the virtual appliance.

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

5 In the Updates pane, click **Check Updates** and select **Check CDROM**.

6 Validate that the loaded Available Updates match the appropriate version, and click **Install Updates** and select **Install all updates**.

7 When the update finishes, click **Summary** to review the updates applied, and then click **Reboot** to cycle the appliance.

8 After the reboot finishes, verify that the appropriate version number has been applied to the appliance.

9 Re-enable traffic to the Platform Services Controller Node 1, and re-enable health monitoring on the load balancer.

   You have applied a patch to first Platform Services Controller instance (Node 1), and re-enabled both network traffic and health monitoring on the load balancer for this node.

10 Repeat this procedure on the second Platform Services Controller (Node 2).

What to do next

If multiple Platform Services Controller HA instances are available in your environment, repeat the preceding procedure for each instance until all Platform Services Controller HA instances have had patches applied.

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 also upgrade the vCenter Server tc Server by using the same patch.

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

Prerequisites

- Download the Java Components patch from VMware downloads page at https://my.vmware.com/group/vmware/patch. The name format is `VMware-VIMPatch-6.5.0-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-6.5.0-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 and the vCenter Server tc Server components are up to date and silently updates them if necessary.

Upgrading ESXi Hosts

8

After you upgrade vCenter Server and vSphere Update Manager, upgrade VMware ESXi hosts. You can upgrade ESXi 5.5.x and ESXi 6.0.x hosts directly to ESXi 6.5.

To upgrade hosts, you can use the tools and methods that are described in Overview of the ESXi Host Upgrade Process.

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:

ESXi Requirements

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

ESXi Hardware Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi6.5.

Hardware and System Resources

To install or upgrade ESXi, 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 6.5 requires a host machine with at least two CPU cores.
- ESXi 6.5 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 6.5 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi 6.5 requires a minimum of 4 GB 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 are considered remote, not local. These disks are not 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 6.5 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 6.5 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.

Starting with vSphere 6.5, VMware Auto Deploy supports network booting and provisioning of ESXi hosts with UEFI.

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

Storage Requirements for ESXi 6.5 Installation or Upgrade

Installing ESXi 6.5 or upgrading to ESXi 6.5 requires a boot device that is a minimum of 1 GB. When booting from a local disk, SAN or iSCSI LUN, a 5.2-GB disk is required to allow for the creation of the VMFS volume and a 4-GB 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 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 is used for an expanded coredump partition on the USB/SD device. Use a high-quality USB flash drive of 16 GB or larger so that the extra flash cells can prolong the life of the boot media, but high-quality drives of 4 GB 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 8-1. Supported Remote Management Server Models and Minimum Firmware Versions

Remote Management Server Model	Firmware Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23

Table 8-1. Supported Remote Management Server Models and Minimum Firmware Versions (continued)

Remote Management Server Model	Firmware Version	Java
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.

Table 8-2. Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host. Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3GB of RAM for baseline performance. This figure includes approximately 1024MB for the virtual machines, 256MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines. These calculations do not take into account possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management*.
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.

Table 8-2. Recommendations for Enhanced Performance (continued)

System Element	Recommendation
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS5 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Web Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. **Note** For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Web Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 6.5 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 and the VMware Host Client allow 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 installed by default. If you install other VIBs on your host, additional services and firewall ports might become available. The information is primarily for services that are visible in the vSphere Web Client but the table includes some other ports as well.

Table 8-3. Incoming Firewall Connections

Port	Protocol	Service	Description
5988	TCP	CIM Server	Server for CIM (Common Information Model).
5989	TCP	CIM Secure Server	Secure server for CIM.
427	TCP, UDP	CIM SLP	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
546		DHCPv6	DHCP client for IPv6.

Table 8-3. Incoming Firewall Connections (continued)

Port	Protocol	Service	Description
8301, 8302	UDP	DVSSync	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.
902	TCP	NFC	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.
12345, 23451	UDP	vSANClustering Service	VMware vSAN Cluster Monitoring and Membership Directory Service. Uses UDP-based IP multicast to establish cluster members and distribute vSAN metadata to all cluster members. If disabled, vSAN does not work.
68	UDP	DHCP Client	DHCP client for IPv4.
53	UDP	DNS Client	DNS client.
8200, 8100, 8300	TCP, UDP	Fault Tolerance	Traffic between hosts for vSphere Fault Tolerance (FT).
6999	UDP	NSX Distributed Logical Router Service	NSX Virtual Distributed Router service. The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open. This service was called NSX Distributed Logical Router in earlier versions of the product.
2233	TCP	vSAN Transport	vSAN reliable datagram transport. Uses TCP and is used for vSAN storage IO. If disabled, vSAN does not work.
161	UDP	SNMP Server	Allows the host to connect to an SNMP server.
22	TCP	SSH Server	Required for SSH access.
8000	TCP	vMotion	Required for virtual machine migration with vMotion. ESXi hosts listen on port 8000 for TCP connections from remote ESXi hosts for vMotion traffic.
902, 443	TCP	vSphere Web Client	Client connections
8080	TCP	vsanvp	vSAN VASA Vendor Provider. Used by the Storage Management Service (SMS) that is part of vCenter to access information about vSAN storage profiles, capabilities, and compliance. If disabled, vSAN Storage Profile Based Management (SPBM) does not work.
80	TCP	vSphere Web Access	Welcome page, with download links for different interfaces.
5900 -5964	TCP	RFB protocol	
80, 9000	TCP	vSphere Update Manager	
9080	TCP	I/O Filter Service	Used by the I/O Filters storage feature

Table 8-4. Outgoing Firewall Connections

Port	Protocol	Service	Description
427	TCP, UDP	CIM SLP	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
547	TCP, UDP	DHCPv6	DHCP client for IPv6.
8301, 8302	UDP	DVSSync	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.
44046, 31031	TCP	HBR	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.
902	TCP	NFC	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.
9	UDP	WOL	Used by Wake on LAN.
12345 23451	UDP	vSAN Clustering Service	Cluster Monitoring, Membership, and Directory Service used by vSAN.
68	UDP	DHCP Client	DHCP client.
53	TCP, UDP	DNS Client	DNS client.
80, 8200, 8100, 8300	TCP, UDP	Fault Tolerance	Supports VMware Fault Tolerance.
3260	TCP	Software iSCSI Client	Supports software iSCSI.
6999	UDP	NSX Distributed Logical 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.
5671	TCP	rabbitmqproxy	A proxy running on the ESXi host. This proxy allows applications that are running inside virtual machines to communicate with the AMQP brokers that are running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. Ensure that outgoing connection IP addresses include at least the brokers in use or future. You can add brokers later to scale up.
2233	TCP	vSAN Transport	Used for RDT traffic (Unicast peer to peer communication) between vSAN nodes.
8000	TCP	vMotion	Required for virtual machine migration with vMotion.

Table 8-4. Outgoing Firewall Connections (continued)

Port	Protocol	Service	Description
902	UDP	VMware vCenter Agent	vCenter Server agent.
8080	TCP	vsanvp	Used for vSAN Vendor Provider traffic.

Table 8-5. Firewall Ports for Services That Are Not Visible in the UI by Default

Port	Protocol	Service	Comment
5900 -5964	TCP	RFB protocol	The RFB protocol is a simple protocol for remote access to graphical user interfaces.
8889	TCP	OpenWSMAN Daemon	Web Services Management (WS-Management is a DMTF open standard for the management of servers, devices, applications, and Web services.

Required Free Space for System Logging

If you used Auto Deploy to install your ESXi 6.5 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 6.5 configures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 8-6. 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.

VMware Host Client System Requirements

Make sure that your browser supports the VMware Host Client.

The following guest operating systems and Web browser versions are supported for the VMware Host Client.

Supported Browsers	Mac OS	Windows	Linux
Google Chrome	75+	75+	75+
Mozilla Firefox	60+	60+	60+
Microsoft Edge	N/A	79+	N/A
Safari	9.0+	N/A	N/A

Before Upgrading ESXi Hosts

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

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 Overview of the ESXi Host Upgrade Process 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 Overview of the ESXi Host Upgrade Process.
   - Make sure that the system hardware complies with ESXi requirements. See ESXi 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 If you are using Auto Deploy to provision hosts, the user who is running the process must have local administrator privileges on the ESXi host that is being provisioned. By default the installation process has these privileges and certificate provisioning happens as expected. However, if you are using another method than the installer, you must run it as a user who has the local administrator privileges.

5 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.

   - For an interactive upgrade from CD, DVD, or USB drive: see Upgrade Hosts Interactively.
   - For a scripted upgrade: see Installing or Upgrading Hosts by Using a Script.
   - For vSphere Auto Deploy: see Chapter 9 Using vSphere Auto Deploy to Reprovision Hosts . If the ESXi 5.5.x or 6.0.x host was deployed by using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a 6.5 image.
   - For the `esxcli` command method: see Upgrading Hosts by Using esxcli Commands .

6 Plan for the tasks that must be performed after the ESXi host upgrade:

   - Test the system to ensure that the upgrade completed successfully.
   - Apply a host's licenses. See Applying Licenses After Upgrading to ESXi 6.5.
   - Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. 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.

7 If the upgrade was unsuccessful and you backed up the host, you can restore the host.

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 5.5.x host or ESXi 6.0.x host to ESXi 6.5, 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.

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 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 PXELINUX 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 using the `mkisofs` or the `genisoimage` command.

Command	Syntax
mkisofs	**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 -eltorito-alt-boot -eltorito-platform efi -b efiboot.img -no-emul-boot /esxi_cdrom**
genisoimage	**genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e efiboot.img -no-emul-boot /esxi_cdrom**

You can use this ISO image for regular boot or UEFI secure boot.

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 can use the preboot execution environment (PXE) to boot a host. Starting with vSphere 6.0, you can PXE boot the ESXi installer from a network interface on hosts with legacy BIOS or using UEFI.

ESXi 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 PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

Sample DHCP Configurations

To PXE boot the ESXi installer, the DHCP server must send the address of the TFTP server and the filename of the initial boot loader to the ESXi host.

When the target machine first boots, it broadcasts a packet across the network requesting information to boot itself. The DHCP server responds. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the initial boot loader binary, typically a file on a TFTP server.

Caution Do not set up a second 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.

Example of Booting Using TFTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi using a TFTP server at IPv4 address xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` or `mboot.efi` binary file on the TFTP server.

Example of Booting Using TFTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi using a TFTP server at IPv6 address xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
```

```
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `mboot.efi` binary file on the TFTP server.

Example of Booting Using HTTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi using a Web server at IPv4 address xxx.xxx.xxx.xxx. The example uses gPXELINUX for legacy BIOS hosts and iPXE for UEFI hosts.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
      } else {
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      filename "gpxelinux.0";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `gpxelinux.0` or `snponly.efi` binary file on the TFTP server. In the UEFI case, iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename.

Example of Booting Using HTTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi using a TFTP server at IPv6 address xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
```

```
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `snponly.efi` (iPXE) binary file on the TFTP server. iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename.

PXELINUX Configuration Files

You need a PXELINUX configuration file to boot the ESXi installer on a legacy BIOS system. The configuration file defines the menu displayed to the target ESXi host as it boots up and contacts the TFTP server for all SYSLINUX configurations, including PXELINUX and gPXELINUX.

This section gives general information about PXELINUX configuration files. For examples, see Sample DHCP Configurations.

For syntax details, see the SYSLINUX web site at http://www.syslinux.org/.

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 in the following order:

1. It tries with the MAC address of the target ESXi host, prefixed with its ARP type code, which is 01 for Ethernet.
2. If that attempt fails, it tries with the hexadecimal notation of target ESXi system IP address.
3. Ultimately, it tries to load a file named `default`.

File Location for the PXE Configuration File

Save the file in `/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 Background Information

Understanding the PXE boot process can help you during troubleshooting.

TFTP Server

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. TFTP is available on Linux and Windows.

- 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. You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.
- If your TFTP server will run on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/.

SYSLINUX, PXELINUX, and gPXELINUX

If you are using PXE in a legacy BIOS environment, you need to understand the different boot environments.

- SYSLINUX is an open source boot environment for machines that run legacy BIOS firmware. The ESXi boot loader for BIOS systems, `mbootc.32`, runs as a SYSLINUX plugin. You can configure SYSLINUX to boot from several types of media, including disk, ISO image, and network. You can find the SYSLINUX package at http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX is a SYSXLINUX configuration for booting from a TFTP server according to the PXE standard. If you use PXELINUX to boot the ESXi installer, the `pxelinux.0` binary file, `mboot.c32`, the configuration file, the kernel, and other files are all transferred by TFTP.
- gPXELINUX is a hybrid configuration that includes both PXELINUX and gPXE and supports booting from a Web server. gPXELINUX is part of the SYSLINUX package. If you use gPXELINUX to boot the ESXi installer, only the `gpxelinux.0` binary file, `mboot.c32`, and the configuration file are transferred via TFTP. The remaining files are transferred via HTTP. HTTP is typically faster and more reliable than TFTP, especially for transferring large amounts of data on a heavily loaded network.

Note VMware currently builds the `mboot.c32` plugin to work with SYSLINUX version 3.86 and tests PXE booting only with that version. Other versions are likely to be incompatible. 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.

UEFI PXE and iPXE

Most UEFI firmware natively includes PXE support that allows booting from a TFTP server. The firmware can directly load the ESXi boot loader for UEFI systems, `mboot.efi`. Additional software such as PXELINUX is not required.

iPXE can also be useful for UEFI systems that do not include PXE in firmware and for older UEFI systems with bugs in their PXE support. For such cases you can try installing iPXE on a USB flash drive and booting from there.

Note Apple Macintosh products do not include PXE boot support. They include support for network booting via an Apple-specific protocol instead.

Alternative Approaches to PXE Booting

Alternative approaches to PXE booting different software on different hosts are also possible, for example:

- Configuring the DHCP server to provide different initial boot loader filenames to different hosts depending on MAC address or other criteria. See your DCHP server's documentation.
- Approaches using iPXE as the initial bootloader with an iPXE configuration file that selects the next bootloader based on the MAC address or other criteria.

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 VMware Customer Connect account at https://my.vmware.com/web/vmware/.

Procedure

1. Log in to VMware Customer Connect.
2. Navigate to **Products and Accounts > All Products**.
3. Find VMware vSphere and click **Download Product**.
4. Select a VMware vSphere version from the **Select Version** drop-down menu.
5. Select a version of VMware vSphere Hypervisor (ESXi) and click **GO TO DOWNLOADS**.
6. Download an ESXi ISO image.
7. Confirm that the md5sum is correct by using an MD5 checksum tool.

Upgrade Hosts Interactively

To upgrade ESXi 5.5 hosts or ESXi 6.0 hosts to ESXi 6.5, 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 an ESXi 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.

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.

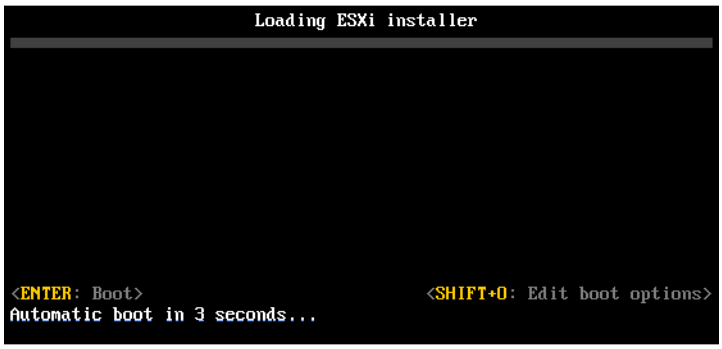
At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See About the boot.cfg File and PXE Booting the ESXi 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 8-7. Boot Options for ESXi Installation

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

Table 8-7. Boot Options for ESXi Installation (continued)

Boot Option	Description
`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`. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

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`. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

`--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 vSAN disk group. If you use this option and no vSAN partition is on the selected disk, the

installation will fail. When you install ESXi on a disk that is in vSAN 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 vSAN 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`. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

`--overwritevsan`

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

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

serialnum or vmserialnum (optional)

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

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

network (optional)

Specifies a network address for the system.

--bootproto=[dhcp|static]	Specifies whether to obtain the network settings from DHCP or set them manually.
--device=	Specifies either the MAC address of the network card or the device name, in the form `vmnicNN`, as in `vmnic0`. This options refers to the uplink device for the virtual switch.
--ip=	Sets an IP address for the machine to be installed, in the form `xxx.xxx.xxx.xxx`. Required with the `--bootproto=static` option and ignored otherwise.
--gateway=	Designates the default gateway as an IP address, in the form `xxx.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--nameserver=	Designates the primary name server as an IP address. Used with the `--bootproto=static` option. Omit this option if you do not intend to use DNS. The `--nameserver` option can accept two IP addresses. For example: `--nameserver="10.126.87.104[,10.126.87.120]"`
--netmask=	Specifies the subnet mask for the installed system, in the form `255.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--hostname=	Specifies the host name for the installed system.
--vlanid= ***vlanid***	Specifies which VLAN the system is on. Used with either the `--bootproto=dhcp` or `--bootproto=static` option. Set to an integer from 1 to 4096.
--addvmportgroup=(0|1)	Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (optional)

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

part or partition (optional)

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

datastore name	Specifies where the partition is to be mounted.
--ondisk= or --ondrive=	Specifies the disk or drive where the partition is created.
--firstdisk= ***disk-type1,*** **[*disk-type2*,...]**	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: 1 Locally attached storage (`local`) 2 Network storage (`remote`) 3 USB disks (`usb`) You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

reboot (optional)

Reboots the machine after the scripted installation is complete.

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

rootpw (required)

Sets the root password for the system.

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

upgrade

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

`--disk= or --drive=`

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

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

For accepted disk name formats, see Disk Device Names.

`--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`. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

%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.

Important The `%firstboot` script does not run, if secure boot is enabled on the ESXi host.

`--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 8-8. 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` or `mboot.efi` 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
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

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

Table 8-9. Commands in `boot.cfg`.

Command	Description
`title=STRING`	Sets the boot loader title to *STRING*.
`prefix=STRING`	(Optional) Adds *DIRPATH/* in front of every *FILEPATH* in the `kernel=` and `modules=` commands that do not already start with / or with `http://`.
`kernel=FILEPATH`	Sets the kernel path to *FILEPATH*.
`kernelopt=STRING`	Appends *STRING* to the kernel boot options.
`modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn`	Lists the modules to be loaded, separated by three hyphens (`---`).

See Create an Installer ISO Image with a Custom Installation or Upgrade Script 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.

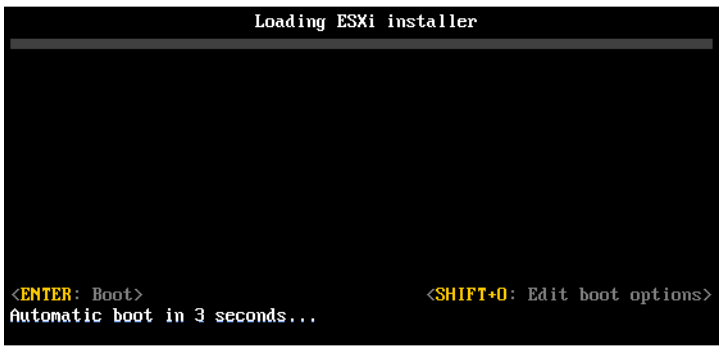
Prerequisites

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 .

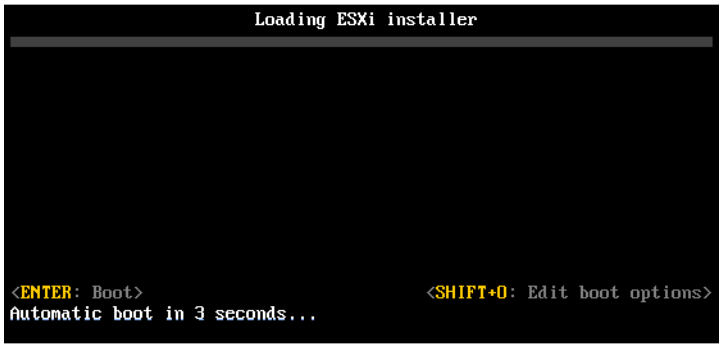
Prerequisites

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 6.5 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 Using a Web Server
  - PXE Boot the ESXi Installer Using TFTP
- For information about using vSphere Auto Deploy to perform a scripted upgrade by using PXE to boot, see Chapter 9 Using vSphere Auto Deploy to Reprovision Hosts .

PXE Booting the ESXi Installer

You can use the preboot execution environment (PXE) to boot a host. Starting with vSphere 6.0, you can PXE boot the ESXi installer from a network interface on hosts with legacy BIOS or using UEFI.

ESXi 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.

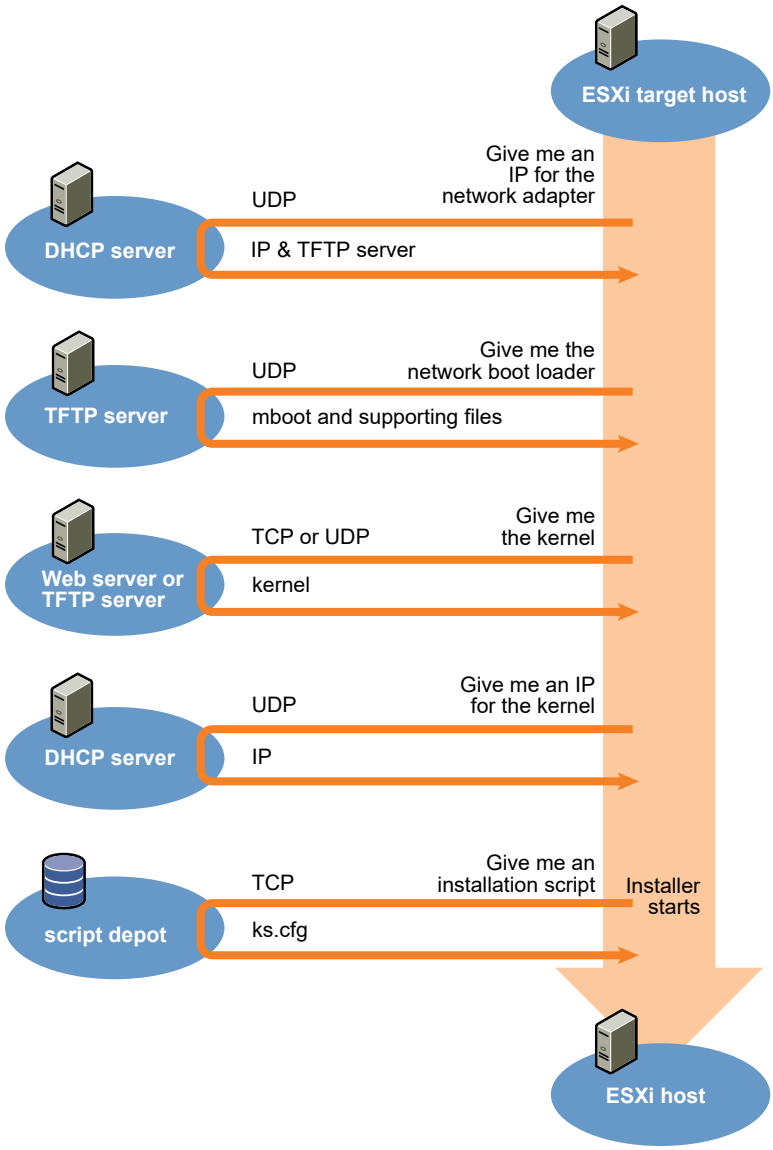
Note PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

Overview of the PXE Boot Installation Process

Some of the details of the PXE boot process vary depending on whether the target host is using legacy BIOS or UEFI firmware, and whether the boot process uses TFTP only or TFTP plus HTTP.

When you boot the target host, it interacts with the different servers in the environment to get the network adapter, boot loader, kernel, IP address for the kernel, and finally the installation script. When all components are in place, installation starts, as shown in the following illustration.

Figure 8-1. Overview of PXE Boot Installation Process



The interaction between the ESXi host and other servers proceeds as follows:

1 The user boots the target ESXi host.

2 The target ESXi host makes a DHCP request.

3 The DHCP server responds with the IP information and the location of the TFTP server.

4 The ESXi host contacts the TFTP server and requests the file that the DHCP server specified.

5 The TFTP server sends the network boot loader, and the ESXi host executes it. The initial boot loader might load additional boot loader components from the TFTP server.

6 The boot loader searches for a configuration file on the TFTP server, downloads the kernel and other ESXi components from the HTTP server or the TFTP server and boots the kernel on the ESXi host.

7 The installer runs interactively or using a kickstart script, as specified in the configuration file.

PXE Boot the ESXi Installer Using TFTP

You can use a TFTP server to PXE boot the ESXi installer. The process differs slightly depending on whether you use UEFI or boot from a legacy BIOS. Because most environments include ESXi hosts that support UEFI boot and hosts that support only legacy BIOS, this topic discusses prerequisites and steps for both types of hosts.

- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` or `gpxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

Prerequisites

Verify that your environment meets the following prerequisites.

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server configured for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).
- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- 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.

For legacy BIOS systems, version 3.86 of the SYSLINUX package, available from https://www.kernel.org/pub/linux/utils/boot/syslinux/.

Procedure

1 Configure the DHCP server for TFTP boot.

2 (Legacy BIOS only) Obtain and configure PXELINUX:

a Obtain SYSLINUX version 3.86, unpack it, and copy the `pxelinux.0` file to the top-level `/tftpboot` directory on your TFTP server.

b Create a PXELINUX configuration file using the following code model.

`ESXi-6.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

c Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server with a filename that will determine whether all hosts boot this installer by default:

Option	Description
Same installer	Name the file `default` if you want for all host to boot this ESXi installer by default.
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*) if you want only a specific host to boot with this file, for example, `01-23-45-67-89-0a-bc`.

3 (UEFI only) Copy the file `efi/boot/bootx64.efi` from the ESXi installer ISO image to `/tftpboot/mboot.efi` on your TFTP server.

Note Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

4 Create a subdirectory of your TFTP server's top-level `/tftpboot` directory and name it after the version of ESXi it will hold, for example, `/tftpboot/ESXi-6.x.x-xxxxx`.

5 Copy the contents of the ESXi installer image to the directory you just created.

6 Modify the `boot.cfg` file

a Add the following line:

```
prefix=ESXi-6.x.x-xxxxxx
```

Here, `ESXi-6.x.x-xxxxxx` is the pathname of the installer files relative to the TFTP server's root directory.

b If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.

7 (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
```

8 (UEFI only) Specify whether you want for all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	a Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. b Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

PXE Boot the ESXi Installer Using a Web Server

You can use a Web server to PXE boot the ESXi installer. Because most environments include ESXi hosts that support UEFI boot and hosts that support only legacy BIOS, this topic discusses prerequisites and steps for both types of hosts.

- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` or `gpxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

Prerequisites

Verify that your environment has the following components:

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server configured for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).

- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- 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.

Verify that your environment also meets the following prerequisites required for PXE boot using a Web Server:

- Verify that the HTTP Web server is accessible by your target ESXi hosts.
- (UEFI) Obtain iPXE, available at http://ipxe.org.
- (Legacy BIOS) Obtain version 3.86 of the SYSLINUX package, available from https://www.kernel.org/pub/linux/utils/boot/syslinux/.

Procedure

1. Configure the DHCP server for HTTP boot.
2. (UEFI only) Obtain and configure iPXE:
   a. Obtain the iPXE source code, as described at http://ipxe.org/download.
   b. Follow the instructions on that page, but use the following make command:

      ```
      make bin-x86_64-efi/snponly.efi
      ```

   c. Copy the resulting file `snponly.efi` to `/tftpboot` directory on your TFTP server.
3. (UEFI only) Copy the file `efi/boot/bootx64.efi` from the ESXi installer ISO image to `/tftpboot/mboot.efi` on your TFTP server.

Note Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

4 (Legacy BIOS only) Obtain and configure PXELINUX:

   a Obtain SYSLINUX version 3.86, unpack it, and copy the `gpxelinux.0` file to the top-level `/tftpboot` directory on your TFTP server.

   b Create a PXELINUX configuration file using the following code model.

   `ESXi-6.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server with a filename that will determine whether all hosts boot this installer by default:

Option	Description
Same installer	Name the file `default` if you want for all host to boot this ESXi installer by default.
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*) if you want only a specific host to boot with this file, for example, `01-23-45-67-89-0a-bc`.

5 Create a directory on your HTTP server named for the version of ESXi it will hold, for example, `/var/www/html/ESXi-6.x.x-XXXXXX`.

6 Copy the contents of the ESXi installer image to the directory you just created.

7 Modify the `boot.cfg` file

   a Add the following line:

```
prefix=http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX
```

   where `http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX` is the location of the installer files on the HTTP server.

   b If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.

8 (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
```

9 (UEFI only) Specify whether you want for all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	a Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. b Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

Upgrading Hosts by Using esxcli Commands

By using vSphere CLI, you can upgrade a ESXi 5.5 host or ESXi 6.0 host to version 6.5 and update or patch ESXi 5.5, ESXi 6.0, and ESXi 6.5 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 8-10. 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 vSAN 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 vSAN 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 machine 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 .

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, Patches, Updates, and Migrations.

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 Overview of the ESXi Host Upgrade Process.

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`** **Important** This is the only update method that VMware supports for zip bundles supplied by VMware. VMware-supplied zip bundle names take the form: **`VMware-ESXi-6.5.0-`*`build_number`*`-depot.zip`** The profile name for VMware-supplied zip bundles takes one of the following forms. ■ **`ESXi-6.5.0-`*`build_number`*`-standard`** ■ **`ESXi-6.5.0-`*`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 .

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 machine 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.

After You Upgrade ESXi Hosts

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 6.5 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 Upgrading Virtual Machines and VMware Tools.
- Set up the vSphere Authentication Proxy service. Earlier versions of the vSphere Authentication Proxy are not compatible with vSphere 6.5. See the *vSphere Security* documentation for details about configuring the vSphere Authentication Proxy service.

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 6.5

After you upgrade to ESXi 6.5, you must apply a vSphere 6.5 license.

When you upgrade ESXi 5.5 or ESXi 6.0 hosts to ESXi 6.5 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 5.5 or 6.0 licenses or acquire vSphere 6.5 licenses from My VMware. After you have vSphere 6.5 licenses, you must assign them to all upgraded ESXi 6.5 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 6.5, you can provide the license key in the kickstart (ks) file.

Run the Secure Boot Validation Script on an Upgraded ESXi Host

After you upgrade an ESXi host from an older version of ESXi that did not support UEFI secure boot, you may be able to enable secure boot. Whether you can enable secure boot depends on how you performed the upgrade and whether the upgrade replaced all of the existing VIBs or left some VIBs unchanged. You can run a validation script after you perform the upgrade to determine whether the upgraded installation supports secure boot.

For secure boot to succeed, the signature of every installed VIB must be available on the system. Older versions of ESXi do not save the signatures when installing VIBs.

UEFI secure boot requires that the original VIB signatures are persisted. Older versions of ESXi do not persist the signatures, but the upgrade process updates the VIB signatures.

- If you upgrade using ESXCLI commands, upgraded VIBs do not have persisted signatures. In that case, you cannot perform a secure boot on that system.
- If you upgrade using the ISO the upgrade process saves the signatures of all new VIBs. This also applies to upgrades of vSphere Update Manager that use the ISO.

If any old VIBs remain on the system the signatures of those VIBs still are not available and secure boot is not possible.

For example, if the system uses a 3rd-party driver, and the VMware upgrade does not include a new version of the driver VIB, then the old VIB remains on the system after the upgrade. In rare cases VMware may drop ongoing development of a specific VIB without providing a new VIB that replaces or obsoletes it, so the old VIB remains on the system after upgrade.

Note

UEFI secure boot also requires an up-to-date bootloader. This script does not check for an up-to-date bootloader.

Prerequisites

- Verify that the hardware supports UEFI secure boot.
- Verify that all VIBs are signed with an acceptance level of at least PartnerSupported. If you include VIBs at the CommunitySupported level, you cannot use secure boot.

Procedure

1. Upgrade the ESXi and run the following command.

   ```
   /usr/lib/vmware/secureboot/bin/secureBoot.py -c
   ```

2. Check the output.

   The output either includes `Secure boot can be enabled` or `Secure boot CANNOT be enabled`.

Required Free Space for System Logging

If you used Auto Deploy to install your ESXi 6.5 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 6.5 configures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 8-11. Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	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

You can use the vSphere Web Client or the `esxcli system syslog` vCLI command to configure the syslog service.

For information about using the `esxcli system syslog` command and other vCLI commands, see *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1. In the vSphere Web Client inventory, select the host.
2. Click **Configure**.
3. Under System, click **Advanced System Settings**.
4. Filter for **`syslog`**.
5. To set up logging globally, select the setting to change and click **Edit**.

Option	Description
Syslog.global.defaultRotate	Maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. Specify the directory 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`.

Option	Description
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 that you want to customize.

   b Click **Edit** and enter the number of rotations and the log size you want.

7 Click **OK**.

Results

Changes to the syslog options take effect immediately.

Using vSphere Auto Deploy to Reprovision Hosts

9

If a host was deployed using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a new image profile that contains a different version of ESXi. You can use vSphere ESXi Image Builder to create and manage image profiles.

Note If you upgrade the host to use an ESXi 6.0 or later image, the vSphere 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. See *vSphere Security*.

The vSphere Auto Deploy server is automatically upgraded if you upgrade the corresponding vCenter Server system. Starting with version 6.0, the vSphere Auto Deploy server is always on the same management node as the vCenter Server system.

This chapter includes the following topics:

Introduction to vSphere Auto Deploy

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

State Information for ESXi Hosts

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

Table 9-1. vSphere Auto Deploy Stores Information for Deployment

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

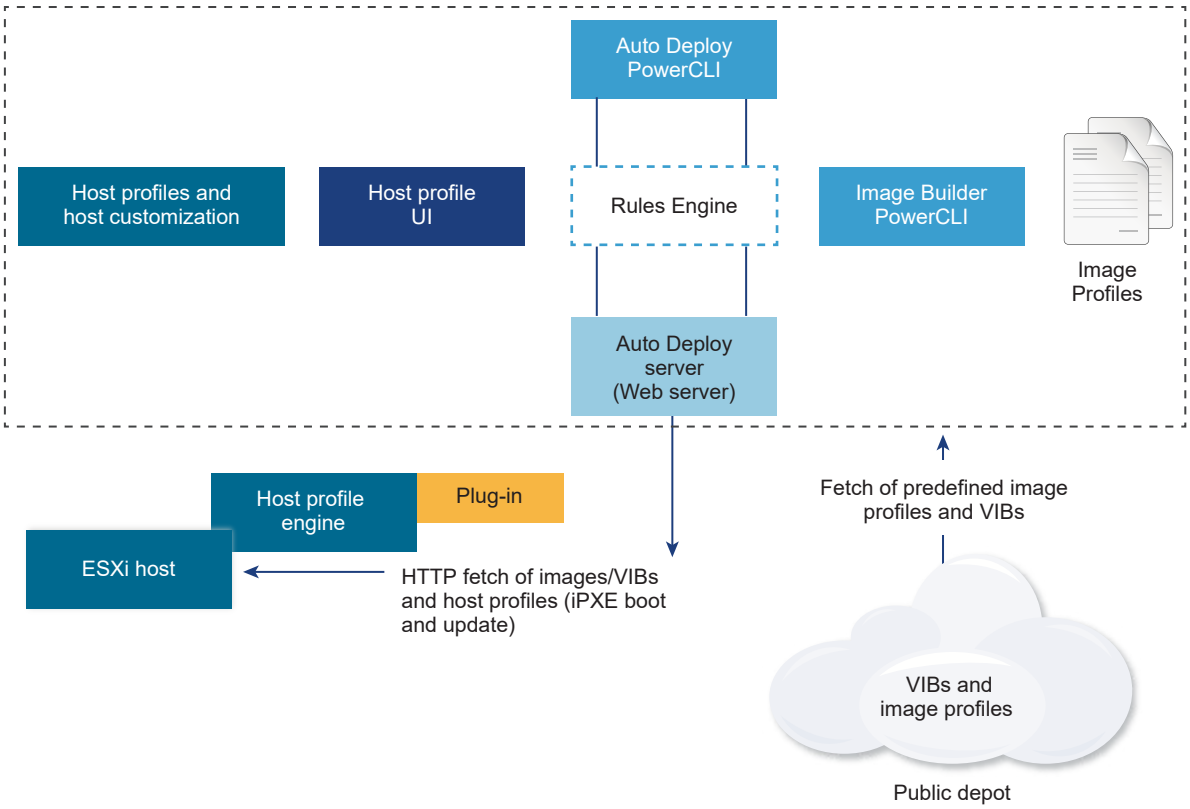
vSphere Auto Deploy Architecture

The vSphere Auto Deploy infrastructure consists of several components.

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

Auto Deploy Architecture
(https://vmwaretv.vmware.com/media/t/1_i4ajkcm2)

Figure 9-1. vSphere Auto Deploy Architecture



vSphere Auto Deploy server

Serves images and host profiles to ESXi hosts.

vSphere Auto Deploy rules engine

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

Image profiles

Define the set of VIBs to boot ESXi hosts with.

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

Host profiles

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

Host customization

Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. For more information about host customizations, see the *vSphere Host Profiles* documentation.

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

Preparing for vSphere Auto Deploy

Before you can start using vSphere Auto Deploy, you must prepare your environment. You start with server setup and hardware preparation. You must configure the vSphere Auto Deploy service startup type in the vCenter Server system that you plan to use for managing the hosts you provision, and install PowerCLI.

- Prepare Your System for vSphere Auto Deploy

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

- Using vSphere Auto Deploy Cmdlets

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

- Set Up Bulk Licensing

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

Prepare Your System for vSphere Auto Deploy

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

For detailed steps and information about preparing your system for vSphere Auto Deploy, see *vSphere Installation and Setup*.

Prerequisites

- Verify that the hosts that you plan to provision with vSphere Auto Deploy meet the hardware requirements for ESXi. See ESXi Hardware Requirements.

- Verify that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met. See Required Ports for vCenter Server and Platform Services Controller.
- If you want to use VLANs in your vSphere Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the firmware driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the UEFI/BIOS interface. You must also correctly configure the ESXi port groups with the correct VLAN IDs. Ask your network administrator how VLAN IDs are used in your environment.
- Verify that you have enough storage for the vSphere Auto Deploy repository. The vSphere Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.

  Best practice is to allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350 MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use.
- Obtain administrative privileges to the DHCP server that manages the network segment you want to boot from. You can use a DHCP server already in your environment, or install a DHCP server. For your vSphere Auto Deploy setup, replace the `gpxelinux.0` file name with `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS. For more information on DHCP configurations, see Sample DHCP Configurations.
- Secure your network as you would for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or the vSphere Auto Deploy server is not checked during a PXE boot.
- If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, verify that Microsoft .NET Framework 4.5 or 4.5.x and Windows PowerShell 3.0 or 4.0 are installed on a Windows machine. You can install PowerCLI on the Windows system on which vCenter Server is installed or on a different Windows system. See the *vSphere PowerCLI User's Guide*.
- Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote Syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.
- Install ESXi Dump Collector, set up your first host so that all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts.

- If the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, verify that the vSphere Auto Deploy server has an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

Procedure

1 Install vCenter Server or deploy the vCenter Server Appliance.

  The vSphere Auto Deploy server is included with the management node.

2 Configure the vSphere Auto Deploy service startup type.

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

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

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

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

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

3 (Optional) If you want to manage vSphere Auto Deploy with the vSphere Web Client, configure the vSphere ESXi Image Builder service startup type.

  a Repeat Substep 2a through Substep 2c.

  b Select **ImageBuilder Service**, click the **Actions** menu, and select **Edit Startup Type**.

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

  c Log out of the vSphere Web Client and log in again.

    The **Auto Deploy** icon is visible on the Home page of the vSphere Web Client.

4 (Optional) If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, install PowerCLI.

   a Download the latest version of PowerCLI from the VMware Web site.

   b Navigate to the folder that contains the PowerCLI file you downloaded and double-click the executable file.

      If the installation wizard detects an earlier version of PowerCLI on your system, it will attempt to upgrade your existing installation

   c Follow the prompts in the wizard to complete the installation.

5 Configure the TFTP server.

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

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

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

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

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

   b Specify the boot file name, which is `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS in the DHCP option 67, frequently called `boot-filename`.

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

8 (Optional) If you set up your environment to use Thumbprint mode, you can use your own Certificate Authority (CA) by replacing the OpenSSL certificate `rbd-ca.crt` and the OpenSSL private key `rbd-ca.key` with your own certificate and key file.

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

   By default, vCenter Server 6.0 and later uses VMware Certificate Authority (VMCA).

Results

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

What to do next

- Define a rule that assigns an image profile and optional host profile, host location or script bundle to the host.
- (Optional) Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- (Optional) If you want to have vSphere Auto Deploy overwrite existing partitions, set up a reference host to do auto partitioning and apply the host profile of the reference host to other hosts.
- (Optional) If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. For more information about host customizations, see the *vSphere Host Profiles* documentation.

Using vSphere Auto Deploy Cmdlets

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

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

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

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

Passing Parameters by Name

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

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

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

Passing Parameters as Objects

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

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

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

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

```
$tr.itemlist
```

3 Remediate the host to use the revised rule set by using the `Repair-DeployRuleSetCompliance` cmdlet with the variable.

```
Repair-DeployRuleSetCompliance $tr
```

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

Set Up Bulk Licensing

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

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

Assign license keys with the vSphere Web Client

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

Assign license keys with LicenseDataManager PowerCLI

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

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

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

Prerequisites

Prepare Your System for vSphere Auto Deploy.

Procedure

1 In a PowerCLI session, connect to the vCenter Server system you want to use and bind the associated license manager to a variable.

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

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

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

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

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

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

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

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

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

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

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

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

Results

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

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 vSphere 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 vSphere Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, custom script, and vCenter Server location.

Prerequisites

- Verify that the setup you performed during the first boot operation is in place.
- Verify that all associated items like are available. An item can be an image profile, host profile, custom script or vCenter Server inventory location.
- Verify that the host has the identifying information (asset tag, IP address) it had during previous boot operations.

Procedure

1 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.

2 Reboot the host.

Results

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

Reprovision a Host with a New Image Profile by Using PowerCLI

You can use vSphere Auto Deploy to reprovision a host with a new image profile in a PowerCLI session 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

- Verify that the image profile you want to use to reprovision the host is available. Use vSphere ESXi Image Builder in a PowerCLI session. See "Using vSphere ESXi Image Builder CLI" in the *vSphere Installation and Setup* documentation.
- Verify that the setup 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 vSphere Auto Deploy is registered with.

```
Connect-VIServer ipv4_or_ipv6_address
```

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 vSphere ESXi Image Builder.

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

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

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

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

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

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

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

   a Verify that you can access the host for which you want to test rule set compliance.

   ```
   Get-VMHost -Name ESXi_hostname
   ```

   b 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 ESXi_hostname
   ```

   c 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 if the host for which you want to test the new rule set compliance is compliant with the active rule set.

   ```
   CurrentItem                          ExpectedItem
   -----------                          ------------
   my_old_imageprofile                        my_new_imageprofile
   ```

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

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

7 Reboot the host to provision it with the new image profile.

Write a Rule and Assign a Host Profile to Hosts

vSphere 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 PowerCLI and all prerequisite software. For information see *vSphere Installation and Setup*.

- Export the host profile that you want to use.

Procedure

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   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` PowerCLI cmdlet, passing in the ESXi host from which you create a host profile.
4. At the 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 vSphere 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 vSphere Auto Deploy rule set or make changes to one or more rules, hosts are not updated automatically. vSphere Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

Prerequisites

- Prepare Your System for vSphere Auto Deploy
- Verify that your infrastructure includes one or more ESXi hosts provisioned with vSphere Auto Deploy, and that the host on which you installed PowerCLI can access those ESXi hosts.

Procedure

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

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

   ```
   Get-DeployRule
   ```

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

3. 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 the active rule set. Instead, you can copy the rule and replace the item or pattern you want to change.

4. Verify that you can access the host for which you want to test rule set compliance.

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

5. 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
   ```

6. 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 if the host for which you want to test the new rule set compliance is compliant with the active rule set.

```
CurrentItem                             ExpectedItem
-----------                             ------------
My Profile 25                           MyNewProfile
```

7 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, reboot your host to have vSphere Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

Changing a vCenter Server Deployment Type After Upgrade or Migration

10

You can change your vCenter Server deployment type after upgrade or migration to version 6.5.

This chapter includes the following topics:

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.
- If you want to repoint a vCenter Server Appliance that is configured in a vCenter HA cluster, remove the vCenter HA configuration. For information about removing a vCenter HA configuration, see *vSphere Availability*.

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 instance is running and can be managed.

Results

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

What to do next

If you repointed a vCenter Server Appliance that was configured in a vCenter HA cluster, you can reconfigure the vCenter HA cluster. For information about configuring vCenter HA, see *vSphere Availability*.

Troubleshooting a vSphere Upgrade

11

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 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 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 `vc-install.txt`, `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 Database Upgrade Logs

You can manually retrieve the database upgrade log files on Microsoft Windows systems for examination.

You can retrieve the database upgrade logs after you finish the vCenter Server upgrade process.

Procedure

1 On the Microsoft Windows system on which you attempted to perform the installation or upgrade, navigate to the database upgrade log locations.

- `%PROGRAMDATA%\VMware\vCenterServer\logs` directory, usually `C:\ProgramData\VMware\vCenterServer\logs`
- `%TEMP%` directory, usually `C:\Users\username\AppData\Local\Temp`

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.

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 11-1. 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 11-1. 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 legacy configuration between reboots.
SUPPORTED_ESX_VERSION	You can upgrade or migrate to ESXi 6.5 only from version 5.5 or 6.0 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 6.5.
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. If you encounter this error, restart the host and retry the upgrade.

vCenter Server Upgrade Might Fail When Stateful ESXi Hosts Are of Version 6.0 or Earlier

Use the present workflows to resolve version compliance errors when upgrading vCenter Server with version 6.0 to version 6.5.

Environment Contains Stateful ESXi 5.1 and 5.5 Hosts

vCenter Server 6.7 does not support host profiles with version earlier than 6.0. Use the present workflow to upgrade your vCenter Server and Host Profiles to version 6.0 or later.

Prerequisites

- Your cluster contains ESXi 5.1 or ESXi 5.5 hosts.
- Your vCenter Server is version 6.0 or 6.5.
- A host profile with version 5.1 or 5.5 is attached to the cluster.

Note Use the PowerCLI commands to fetch the list of host profiles with version less than 6.0 in thevCenter Server inventory: `Get-VMHostProfile | % { $_.ExtensionData.Config.ApplyProfile.ProfileVersion +"`t"+ $_.Name }`

Or

```
Get-VMHostProfile | ?
{ $_.ExtensionData.Config.ApplyProfile.ProfileVersion -like "5*" }
```

Note List of unsupported host profiles with version less than 6.0 in the installer log can be found at: `/var/log/vmware/upgrade/vcdb_req.err` when upgrade fails at pre-check.

Procedure

1. Leave one ESXi host with version 5.1 or 5.5 and upgrade the rest of the ESXi hosts in the cluster to the same version as your vCenter Server.

   When a reference host with version 5.1 or 5.5 is present, you can edit a host profile with the same version.

2. If the ESXi hosts have been added to the Active Directory domain before the upgrade, edit the host profile with version 5.1 or 5.5 and disable the Active Directory profile.

3. Apply the host profile to the cluster.

   The host profile gets applied to all the hosts in the cluster, including to the host with version 5.1 or 5.5.

4. (Optional) Join one of the upgraded hosts to the Active Directory domain.

   If you encounter `objectNotFound` error:

   a Right-click on the host and disconnect it.

   b Reconnect the host to the vCenter Server and join the host to the Active Directory domain.

   The Active Directory settings configured in the ESXi host before the upgrade are not retained when the host is upgraded to vCenter Server 6.0. The host is no longer joined to the domain. After the upgrade, you have to rejoin the hosts to the Active Directory domain.

5 Extract a new host profile from one of the upgraded hosts.

Note If any of the upgraded hosts is part of the Active Directory domain, extract a new host profile from it.

6 Upgrade the ESXi host with version 5.1 or 5.5 to the same version as your vCenter Server.

7 Attach the newly extracted host profile to the cluster.

There might be a change in the host profiles behavior and policy options. For more information, see *Host Profiles Upgrade Workflows*.

The host customization data auto-populates (except for security-related options).

8 Remediate the cluster with the attached host profile.

9 Remove all host profiles with version 5.1 or 6.0 from the vCenter Server inventory.

10 (Optional) If hosts are part of Distributed Virtual Switch (DVS) with version 5.1 or 6.0, upgrade the DVS to the same version as your vCenter Server.

What to do next

Proceed with upgrading the vCenter Server to version 6.7. For more information, see *Recommended Host Profiles Upgrade Workflows.*

Environment Contains Stateful ESXi 6.5 Hosts Only

If your cluster contains stateful ESXi 6.0 hosts, you use the present workflow to resolve version compliance errors when upgrading vCenter Server 6.0 to version 6.5.

It is recommended to upgrade your host profiles to the same version as your vCenter Server.

Prerequisites

- Your cluster contains ESXi 6.0 hosts.
- Your vCenter Server is with version 6.0.
- A host profile with version 6.0 is attached to the cluster.

Procedure

1 Upgrade your vCenter Server to version 6.5.

There are no changes in the vCenter Server configurations.

2 Upgrade all ESXi hosts in the cluster to version 6.5.

Edit host customization and host profile edit operations are not available, see KB 2150534. Compliance check, attach host profile and remediate hosts operations are available.

3 (Optional) Leave one ESXi host at version 6.0, to use your current host profiles version 6.0.

4 Remediate the ESXi hosts in the cluster against the host profile with version 6.0.

All host profile settings are applied.

5 (Optional) Skip the next steps, to use your current host profiles version 5.5.

6 Extract a new host profile from an ESXi 6.5 host.

There are some changed parameters for the host profile policy. For more information, see Answer File Field and Host Profile Extraction.

7 Attach the host profile with version 6.5 to the cluster.

The host customization data auto-populates.

All host profile operations are available.

What to do next

Proceed with upgrading the vCenter Server to version 6.7. For more information, see *Recommended Host Profiles Upgrade Workflows.*

vCenter Server Upgrade Might Fail When Stateless ESXi Hosts Are of Version 6.0 or Earlier

Use the present workflows to resolve version compliance errors when upgrading vCenter Server with version 6.0 to version 6.5.

Environment Contains Stateless ESXi 5.1 and 5.5 Hosts

vCenter Server 6.7 does not support host profiles with version earlier than 6.0. Use the present workflow to upgrade your vCenter Server and Host Profiles to version 6.0 or later.

Prerequisites

- Your cluster contains ESXi 5.1 or ESXi 5.5 hosts.
- Your vCenter Server is version 6.0 or 6.5.
- A host profile with version 5.1 or 5.5 is attached to the cluster.

Note Use the PowerCLI commands to fetch the list of host profiles with version less than 6.0 in thevCenter Server inventory: `Get-VMHostProfile | % { $_.ExtensionData.Config.ApplyProfile.ProfileVersion +"`t"+ $_.Name }`

Or

```
Get-VMHostProfile | ?
{ $_.ExtensionData.Config.ApplyProfile.ProfileVersion -like "5*" }
```

Note List of unsupported host profiles with version less than 6.0 in the installer log can be found at: `/var/log/vmware/upgrade/vcdb_req.err` when upgrade fails at pre-check.

Procedure

1 Create a rule with image profile version 6.0.

2 Activate the rule for all the ESXi hosts version 5.1 or 5.5 in the cluster.

3 If the host profile contains an Active Directory profile, edit the host profile and disable the Active Directory.

   The Active Directory settings configured in the ESXi host are not retained when the host is upgraded to ESXi 6.0.

4 Boot one of the hosts with version 5.1 or 5.5 by using the newly created rule.

   The host boots from the image profile with version 6.0 and from the host profile that is attached to the cluster.

   The host is upgraded to ESXi 6.0. If the host has been added to the Active Directory domain before the upgrade, it is no longer joined to this domain.

5 (Optional) If needed, join the upgraded host back to the Active Directory domain.

6 Extract a new host profile from the upgraded host.

7 Boot the remaining hosts with version 5.1 or 5.5 from the vCenter Server inventory.

   All the hosts are upgraded to version 6.0.

8 Attach the newly extracted host profile to the cluster.

   There might be a change in the host profiles behavior and policy options. For more information, see *Host Profiles Upgrade Workflows*.

   The host customization data auto-populates (except for security-related options).

9 Remediate the cluster with the attached host profile.

10 Remove all host profiles with version 5.1 or 6.0 from the vCenter Server inventory.

11 (Optional) If hosts are part of Distributed Virtual Switch (DVS) with version 5.1 or 6.0, upgrade the DVS to the same version as your vCenter Server.

What to do next

Proceed with upgrading the vCenter Server to version 6.7. For more information, see *Recommended Host Profiles Upgrade Workflows.*

Environment Contains Stateless ESXi 6.0 Hosts Only

If your cluster contains stateful ESXi 6.0 hosts, you use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.0 to version 6.5.

It is recommended to upgrade your host profiles to the same version as your vCenter Server.

Prerequisites

- Your cluster contains ESXi 6.0 hosts.
- Your vCenter Server is with version 6.0.
- A host profile with version 6.0 is attached to the cluster.

Procedure

1. Create a host profile from an ESXi 6.0 host.
2. Apply the host profile to the cluster.
3. Upgrade your vCenter Server to version 6.5.

   There are no changes in the vCenter Server configurations.
4. Create a rule with an image profile version 6.5 and select the cluster.
5. Activate the rule.
6. Boot all ESXi hosts in the cluster.

   All hosts are compliant with the host profile.

   Remediation and check that compliance operations are available, but the host profile with version 6.0 cannot be edited.

   Note Skip the next steps, to use your current host profiles version 6.0.

   The hosts boot using the new rule and the new host profile is applied.
7. (Optional) Extract a new host profile from an ESXi 6.5 host.

   There are some changed parameters for the host profile policy. For more information, see Answer File Field and Host Profile Extraction.
8. (Optional) Attach the host profile with version 6.5 to the cluster.

   The host customization data auto-populates.

   All host profile operations are available.

What to do next

Proceed with upgrading the vCenter Server to version 6.7. For more information, see *Recommended Host Profiles Upgrade Workflows.*

Restore vCenter Server 5.5 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 5.5), it might not reregister vCenter Inventory Service or other vCenter Server services with the vCenter Single Sign-On included in Platform Services Controller 6.5.

Cause

vCenter Inventory Service and other vCenter Server services are unregistered from vCenter Single-Sign-On 5.5 during the upgrade to vCenter Server 6.5. If an upgrade failure occurs after the services are unregistered, the registration information is lost. When the upgrade to vCenter Server 6.5 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 6.5 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.

Roll Back a vCenter Server Instance on Windows When vCenter Server Upgrade Fails

You can roll back or restore a vCenter Server instance on Windows when an upgrade of vCenter Server with an external Platform Services Controller fails after the export stage and the legacy environment has been uninstalled.

Prerequisites

The roll back or restore of vCenter Server applies when all of the following conditions apply:

- You must have access to the vCenter Server on Windows machine.
- The vCenter Server instance is attached to an external Platform Services Controller.
- The Platform Services Controller upgrade must be successful.
- The upgrade of the vCenter Server instance attached to the Platform Services Controller instance is in a failed state after the export stage and uninstallation of the legacy vCenter Server.
- Ensure that vCenter Server rollback happened properly in case of upgrade failure and that no stale failed upgrade log entries remain.

For Rollback Method 1:

- To unregister vCenter Server 6.0.x from the Platform Services Controller, see KB 2106736.
- Use a Platform Services Controller snapshot taken after the Platform Services Controller node upgrade and before the start of the vCenter Server upgrade.
- Use a vCenter Server snapshot taken after the Platform Services Controller upgrade and before the start of the vCenter Server upgrade.
- Use a vCenter Server database snapshot taken after the Platform Services Controller upgrade and before the start of the vCenter Server upgrade.

For Rollback Method 2:

- Use a powered off snapshot of the vCenter Server after the Platform Services Controller upgrade and before the vCenter Server upgrade.

Procedure

- You can restore the legacy vCenter Server using Rollback Method 1 or Rollback Method 2.
  - Use Rollback Method 1.
    a. Manually unregister the legacy vCenter Server from the Platform Services Controller.
    b. Restore the vCenter Server database from a backup which was taken before the upgrade.
    c. Reinstall the vCenter Server instance pointing to the Platform Services Controller and also pointing to the database with the restored data.
    d. Ensure that the vCenter Server services are up and running.
  - Use Rollback Method 2.
    a. Restore the Platform Services Controller instance from a snapshot to the point where you were about to start vCenter Server upgrade. You can use a backup for a Windows configuration or use another backup and restore approach to revert the snapshot.
    b. Restore the vCenter Server instance from a snapshot.
    c. Restore the vCenter Server database from a snapshot.
    d. Ensure that the vCenter Server services are up and running.

  For Rollback Method 2, you will lose all data written to Platform Services Controller after the vCenter Server upgrade has been started when you restore from the Platform Services Controller snapshot taken before that point in time.

VMware Component Manager Error During Startup After vCenter Server Appliance 5.5 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 6.5 upgrade.

Solution

See Upgrade a vCenter Server Appliance 5.5 or 6.0 with an Embedded vCenter Single Sign-On or Platform Services Controller by Using the GUI.

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?.

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.