vCenter Server Upgrade

Update 2
11 APR 2019
VMware vSphere 6.7
vCenter Server 6.7

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About vCenter Server Upgrade

1

vCenter Server Upgrade describes how to upgrade VMware vCenter Server™ to the current version.

To move to the current version of vCenter Server by performing a fresh installation that does not preserve the existing configuration of your environment, see the *vCenter Server Installation and Setup* documentation.

Intended Audience

vCenter Server Upgrade is for anyone who must 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.

vCenter Server Upgrade Options

2

vCenter Server 6.7 provides many options for upgrading your vCenter Server deployment. For a successful vCenter Server 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.

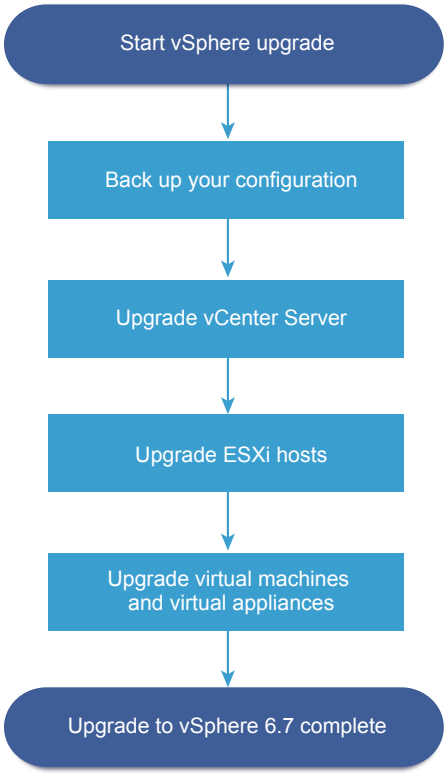
Important You cannot change your vCenter Server deployment type during upgrade.

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 2-1. 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 If your vSphere system includes Platform Services Controller, upgrade Platform Services Controller appliance 6.0 to version 6.7.

5 Upgrade vCenter Server.

See Overview of the vCenter Server Upgrade Process.

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

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.

   For detailed instructions, see *ESXi Upgrade*.

8 Upgrade your VMs and virtual appliances, manually or by using vSphere Update Manager, to perform an orchestrated upgrade.

   For detailed instructions, see *ESXi Upgrade*.

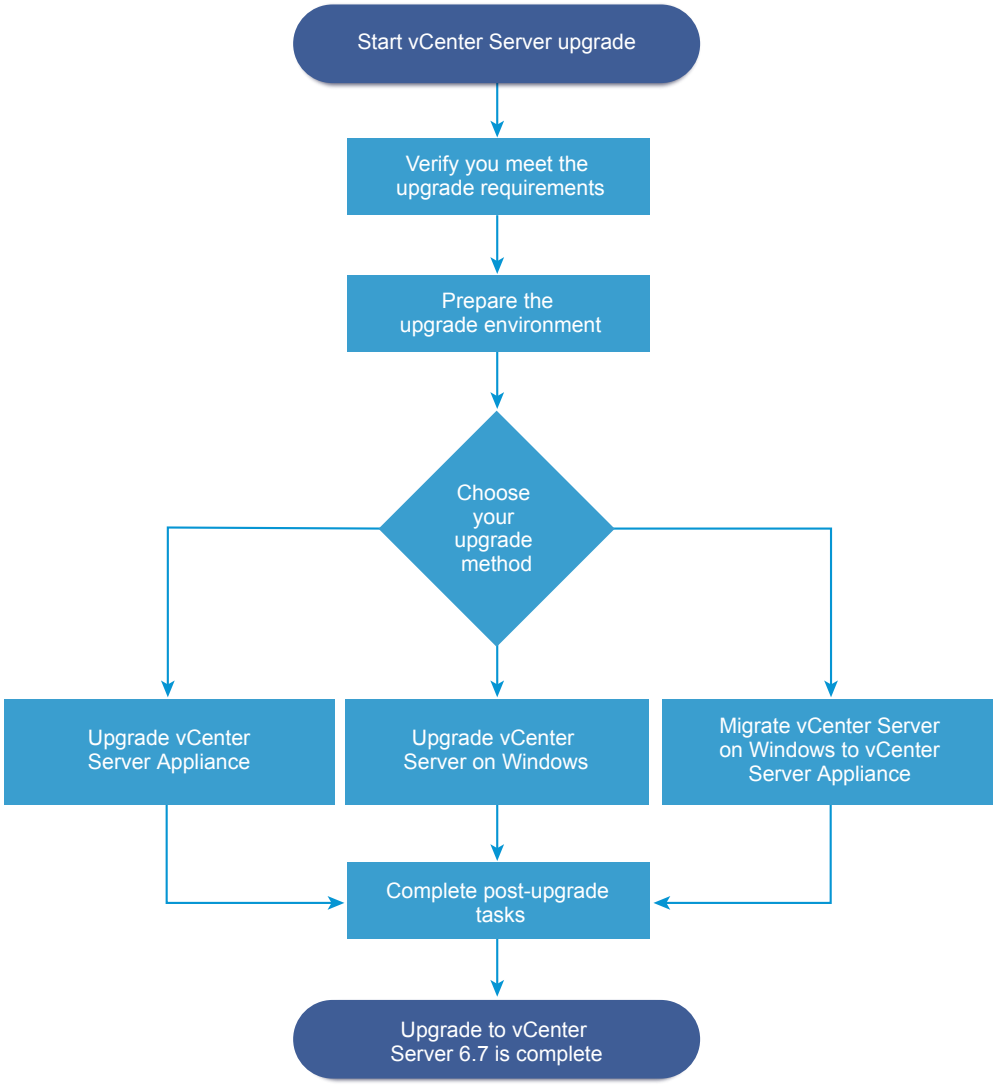
When you upgrade vSphere, you must perform all procedures in sequence to avoid possible data loss and to minimize downtime. You can perform the upgrade process for each component in only one direction. For example, after you upgrade to vCenter Server 6.7, you cannot revert to vCenter Server version 6.0 or version 6.5. 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 6.7.

You can upgrade or migrate your vCenter Server version 6.0 or version 6.5 installation to version 6.7 using the method that best addresses your deployment goals and requirements.

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



High-level steps for upgrading or migrating vCenter Server:

1 Select your upgrade goal.

- Chapter 4 Upgrading the vCenter Server Appliance and Platform Services Controller Appliance
- Chapter 3 Upgrading vCenter Server for Windows
- Chapter 5 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. 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 an OVA file that you deploy, 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 6.7 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 6.7 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 6.7 deployment. See Differences Between vSphere Upgrades, Patches, Updates, and Migrations and Chapter 8 Patching and Updating vCenter Server 6.7 Deployments.

vCenter Server Upgrade Compatibility

The upgrade to vCenter Server 6.7 affects other software components of the data center.

Table 2-1 summarizes how upgrading vCenter Server can affect your data center components.

vCenter Server 6.7 can manage ESXi version 6.0 or 6.5 hosts in the same cluster with ESXi 6.7 hosts vCenter Server 6.7 cannot manage ESXi 5.5 or earlier hosts.

vSphere supports upgrades from vCenter Server 6.0 and later to vCenter Server 6.7. To upgrade from vCenter Server 5.0, 5.1 or 5.5, you must first upgrade the vCenter Server instance to version 6.0 or later releases, and then upgrade to vCenter Server 6.7. For information about upgrading vCenter Server 5.0, 5.1, or 5.5 to version 6.0 or 6.5, see the *VMware vSphere 6.0 Documentation* or *VMware vSphere 6.5 Documentation*

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

Product or Component	Compatibility
vCenter Server	Verify support for the upgrade path from your current version of vCenter Server to your planned upgrade version. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
vCenter Server database	Verify that your database is supported for the vCenter Server version that you are upgrading to. Upgrade the database if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. **Note** vCenter Server Appliance for version 6.7 uses PostgreSQL for the embedded database. vCenter Server Appliance 6.7 does not support external databases.
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. vCenter Server 6.7 requires ESXi host version 6.0 or later. Upgrade if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
VMware Host Profiles	Host Profiles is a vCenter Server tool for designing and deploying ESX and ESXi hosts. Ensure that you are using Host Profiles version 6.0 or later. See Knowledge Base article KB 52932. For more information on upgrade problems related to Host Profiles, see Upgrade Issues with vCenter Server Containing Host Profiles and the sections on Host Profiles upgrade workflows in the *vSphere Host Profiles* documentation.
VMFS3 volumes	ESXi and vCenter Server supports VMFS3, VMFS5, and VMFS6 datastores. You can continue to use existing VMFS3 datastores, but you cannot create new VMFS3 datastores. If you have VMFS3 datastores, upgrade them to VMFS6. For more information on VMFS datastores, see the *vSphere Storage* documentation.
Virtual machines	Upgrade options depend on your current version. See the information about upgrading virtual machines in the *ESXi Upgrade* documentation.
VMware Tools	Upgrade options depend on your current version. See the information about upgrading VMware Tools in the *ESXi Upgrade* documentation.

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

Product or Component	Compatibility
Auto Deploy	To ensure compatibility and best performance, when you upgrade to vCenter Server 6.7, use Auto Deploy to upgrade ESXi hosts to the same version.
vSphere Distributed Virtual Switch (DVS)	You must upgrade to DVS version 6.0 or later before you upgrade to vCenter Server 6.7. See Knowledge Base article KB 52826.
vSphere Network I/O Control	DVS version 6.0 or later supports only Network I/O Control version 3. If you are using an earlier version of Network I/O Control you must upgrade to Network I/O Control version 3. For more information, see the *vSphere Networking* documentation.
vSAN	To avoid potential faults because of differences in the vSAN support in vCenter Server and ESXi, synchronize versions of vCenter Server and ESXi. For the best integration between vSAN components on vCenter Server and ESXi, deploy the latest version of these two vSphere components. For more information, see the *ESXi Installation and Setup*, *vCenter Server Installation and Setup*, *ESXi Upgrade*, and *vCenter Server Upgrade* documentation.
vSAN disk version	vSAN has several different on-disk format versions available depending on the version and upgrade history of the cluster. Some on-disk format versions are transient while others are intended for long-term production. As certain vSAN features are tied to the on-disk format version, the format version must be accounted for when determining interoperability. See Knowledge Base article KB 2145267.
Legacy Fault Tolerance	If the vCenter Server inventory contains a VM on which legacy VMware Fault Tolerance (FT) is in use, upgrade or migration will be blocked until you turn off this feature. For information about legacy FT, see Knowledge Base article KB 2143127. For information on disabling or turning off FT, see Knowledge Base article KB 1008026.

vSphere 6.7 Component Behavior Changes that Affect Upgrade

When upgrading to vSphere 6.7, it is important to understand changes in component behavior for version 6.7 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 6.7, see the Release Notes for version 6.7 releases.

vCenter Server Upgrade Methods

vSphere supports multiple methods for upgrading vCenter Server to version 6.7.

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 6.7 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 6.7 using a CLI. See CLI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance.
Auto Deploy Changes	You can use a graphical user interface (GUI) for upgrading vCenter Server deployments that were initially set up with Auto Deploy.
VMware Update Manager Changes	You can use a graphical user interface (GUI) when upgrading vCenter Server deployments using VMware Update Manager.
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.

Topology Changes After Upgrade or Migration	You can change your deployment topology after upgrade or migration to vCenter Server 6.7. You cannot change your deployment type during upgrade or migration. For information on supported topology changes, see 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 or 6.5 to 6.7 is supported for pure IPv4 or pure IPv6 management networks only.

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

Table 2-2. 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 6.7. The maximum inventory size that applied for Microsoft SQL Server Express still applies for PostgreSQL.

vCenter Inventory Services Removed for vCenter Server 6.7

vCenter Inventory Services are no longer needed for vCenter Server 6.7. 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 Platform Services Controller 6.0 and 6.5 instances first. You temporarily leave the vCenter Server instances at version 6.0 or version 6.5 while you complete the upgrade or migration process for thePlatform Services Controller 6.0 or 6.5 instances.

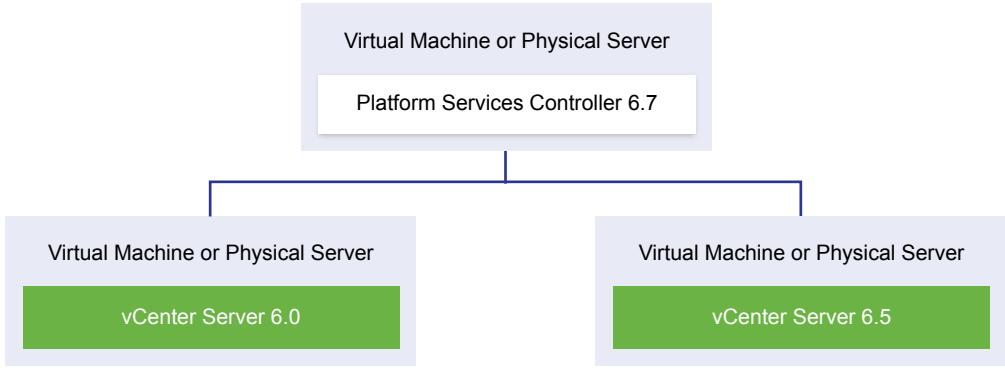
- You must upgrade or migrate your Platform Services Controller 6.0 or 6.5 instances sequentially.
- For a mixed-platform installation with Platform Services Controller 6.0 or 6.5 instances on Windows and vCenter Server Appliance instances, upgrade or migrate all the Platform Services Controller 6.0 or 6.5 instances on Windows before upgrading any vCenter Server Appliance instances.
- For a mixed-platform installation with Platform Services Controller 6.0 or 6.5 appliances and vCenter Server instances on Windows, upgrade all Platform Services Controller 6.0 or 6.5 appliances before upgrading or migrating any vCenter Server instances on Windows.
- After upgrading or migrating your Platform Services Controller 6.0 or 6.5 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 Platform Services Controller 6.0 instance to an externally deployed Platform Services Controller 6.7 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 6.7 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 vCenter Server Appliance environments.

Figure 2-3. Mixed-Version 6.0 and 6.7 Transitional Environment



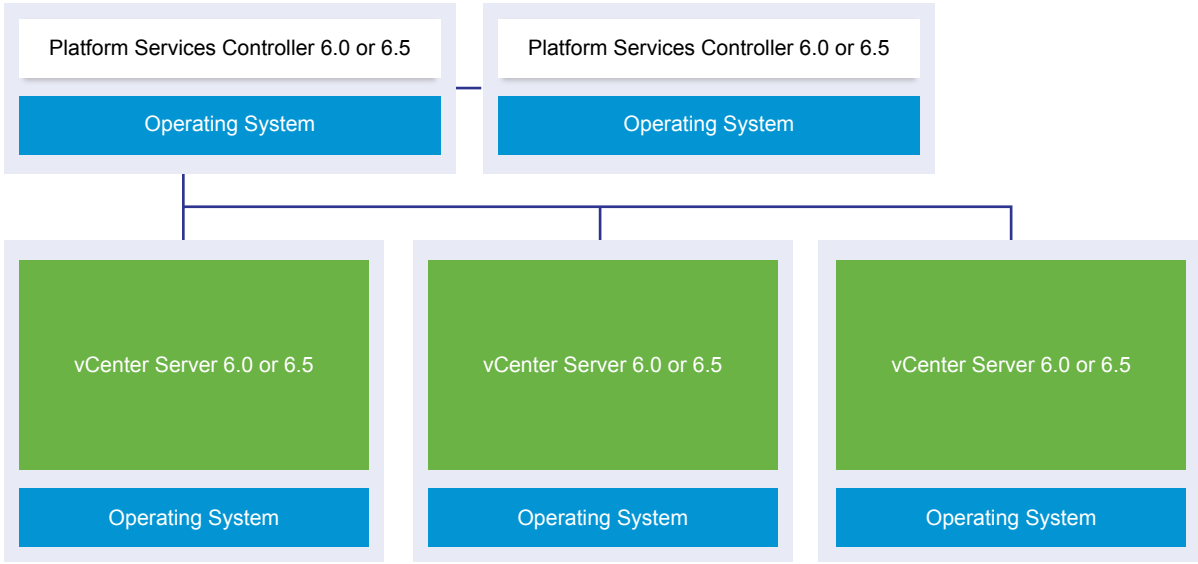
Important Mixed-version environments are not supported for production. Use these environments only during the period when an environment is in transition between vCenter Server versions.

The transitional order and behavior are the same for vCenter Server 6.0 or 6.5 environments when upgrading or migrating to vCenter Server 6.7 environments. The vCenter Server 6.0 instances continue operating with the Platform Services Controller 6.7 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.

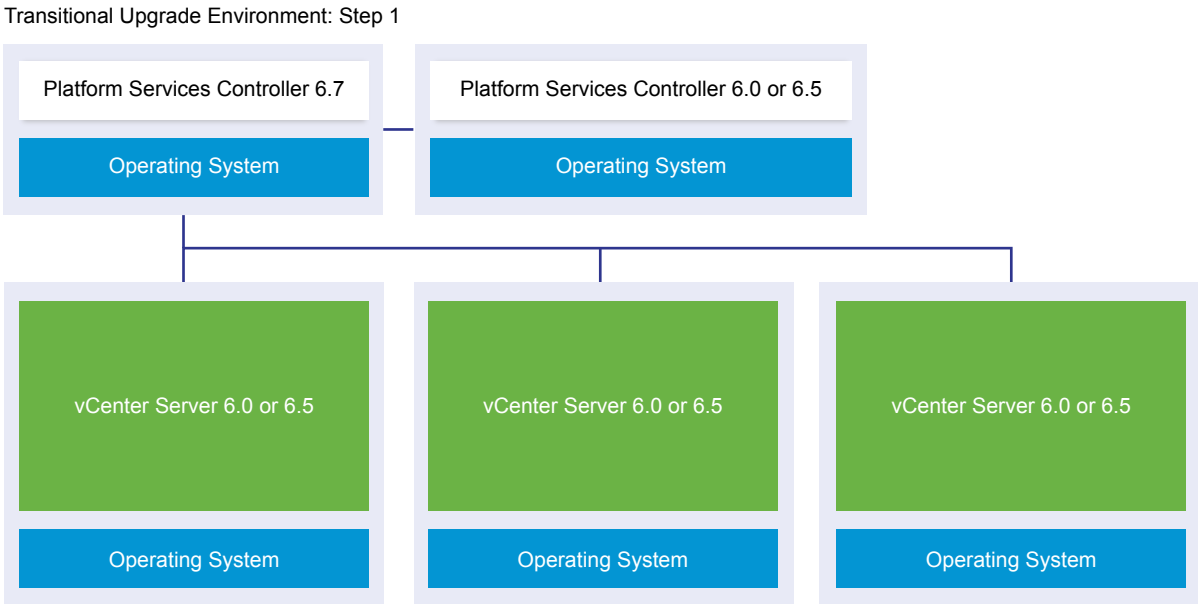
Figure 2-4. Example vSphere 6.0 or 6.5 Deployment Before Transition Begins

Transitional Upgrade Environment: Start



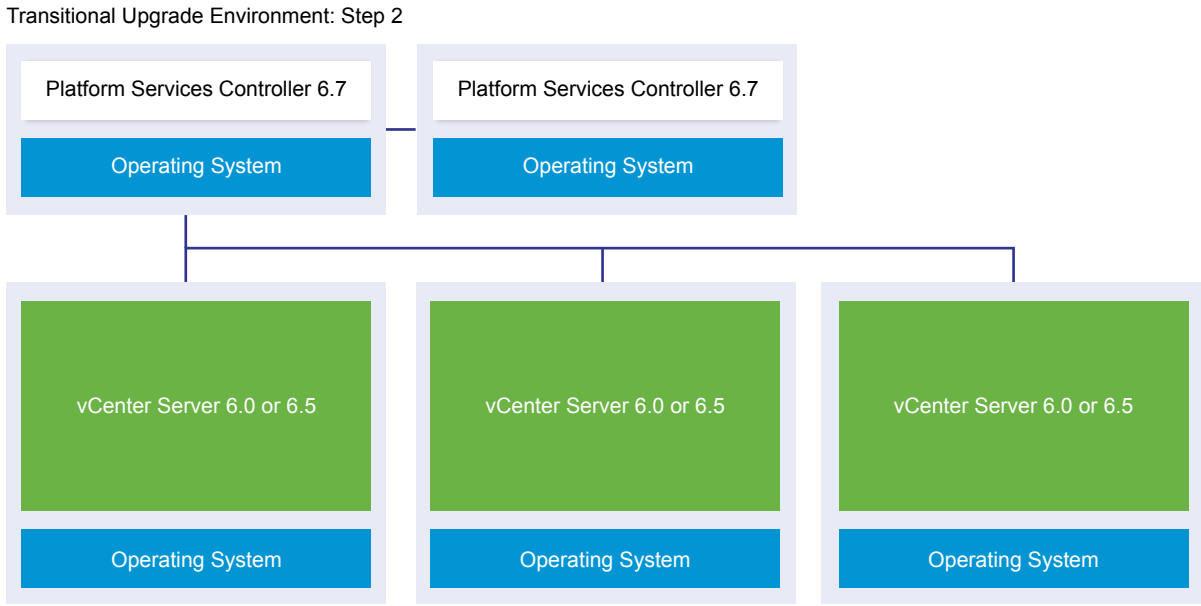
For example, a deployment with three vCenter Server instances and two external vCenter Single Sign-On instances must be upgraded or migrated one instance at a time to version 6.7.

Figure 2-5. Example vSphere 6.0 or 6.5 Deployment in Transition at Step 1



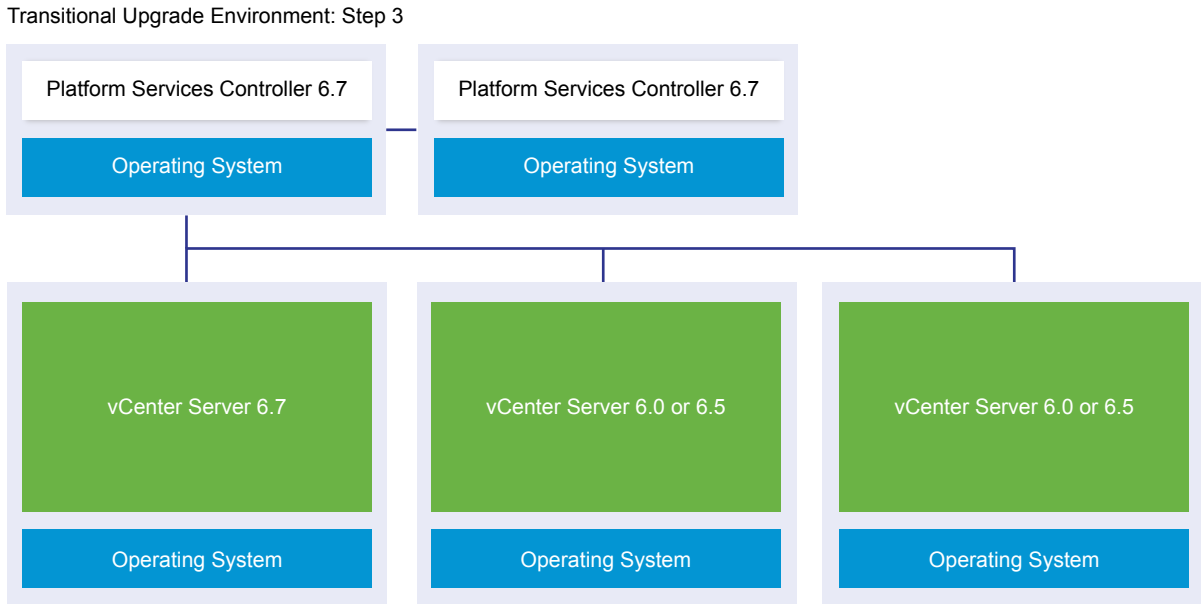
Upgrading or migrating the first external vCenter Single Sign-On instance or Platform Services Controller instance to an external Platform Services Controller of the current version has no impact on the legacy vCenter Server instances.

Figure 2-6. Example vSphere 6.0 or 6.5 Deployment in Transition at Step 2



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

Figure 2-7. Example vSphere 6.0 or 6.5 Deployment in Transition at Step 3



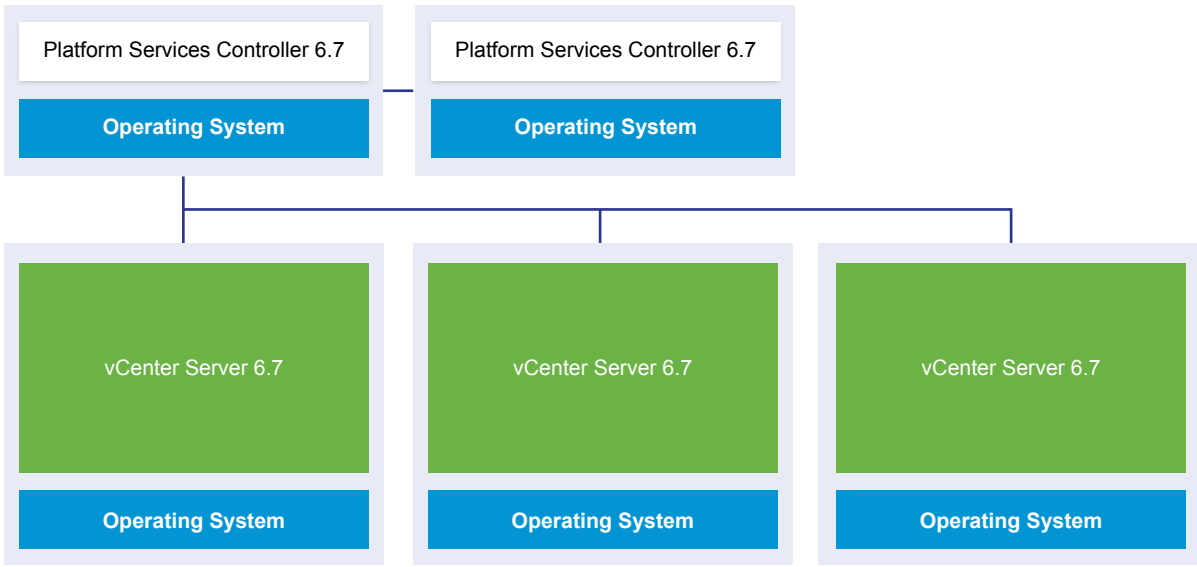
After upgrading the first vCenter Server instance to 6.7, changes occur in the connectivity between the vCenter Server instances.

- The two remaining legacy vSphere Web Client instances can no longer view the newly upgraded vCenter Server 6.7 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 6.7 instance that is part of the newly upgraded vCenter Server 6.7 instance can view the legacy vCenter Server instances and 6.7 instances.

After upgrading the second vCenter Server instance to 6.7, 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 6.7 instances after they are joined to the Platform Services Controller.
- The remaining legacy vSphere Web Client instance can no longer view the vCenter Server 6.7 instances.
- The legacy vSphere Web Client instance can still view the legacy vCenter Server instances after they are restarted.
- The vSphere Web Client 6.7 instances that are part of the newly upgraded vCenter Server 6.7 instances can view the legacy vCenter Server instances and 6.7 instances.

Figure 2-8. Example vSphere 6.0 Deployment After Step 5 with Upgrade Complete



After upgrading the third and final vCenter Server instance to 6.7, all the vCenter Server instances are connected with full vCenter Server 6.7 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 6.7 instances.
- The vSphere Web Client 6.7 instances can view all the vCenter Server 6.7 instances.

Differences between Upgrading and Migrating vCenter Server on Windows

You have two choices for moving your vCenter Server deployment on Windows to version 6.7: 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 6.7.

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 6.0 or version 6.5 deployment on Windows to a vCenter Server 6.7 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 6.0 or version 6.5 deployment on Windows to a vCenter Server Appliance 6.7 deployment. For details, see Chapter 5 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 6.7:

- vCenter Server with an embedded Platform Services Controller (version 6.0 or 6.5)
- vCenter Server with an external Platform Services Controller (version 6.0 or 6.5)

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 Platform Services Controller (version 6.0 or 6.5), the migration is a single workflow.
- When migrating vCenter Server with an external Platform Services Controller (version 6.0 or 6.5), migration order matters. You migrate Platform Services Controller instances before migrating vCenter Server instances. For details, see Chapter 5 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 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 6.7. A release that changes either digit, for example, from 6.0 to 6.5, or from 6.5 to 6.7, 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 4 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 8 Patching and Updating vCenter Server 6.7 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 information, see the *ESXi Upgrade* documentation.

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 5 Migrating vCenter Server for Windows to vCenter Server Appliance.

Support for Federal Information Processing Standard 140-2

vCenter Server 6.7 supports Federal Information Processing Standard (FIPS) 140-2.

FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. By default, FIPS 140-2 is always enabled after installation or upgrade of vCenter Server 6.7.

To learn more about support for FIPS 140-2 in VMware products, see https://www.vmware.com/security/certifications/fips.html.

To learn how to enable or disable FIPS 140-2 support, see the *vSphere Security* documentation.

Support for Transport Security Layer 1.2

By default, vSphere 6.7 supports the Transport Security Layer (TLS) 1.2 encryption protocol. The upgrade or migration to vCenter Server 6.7 disables the TLS 1.0 and TLS 1.1 encryption protocols, and you may need to reconfigure other VMware products and third-party products to use TLS 1.2.

During both upgrade and migration from vCenter Server 6.0 and 6.5 to vCenter Server 6.7, a notification message informs you that only the TLS 1.2 protocol is enabled. If you need to use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, you can use the TLS Configurator Utility to enable or disable the different TLS protocol versions. You can disable TLS 1.0, or you can disable both TLS 1.0 and TLS 1.1.

When upgrading a Platform Services Controller instance that manages one or more vCenter Server 6.0 or 6.0U1 instances which rely on the older protocols, TLS 1.0 and TLS 1.1 remain enabled to avoid a loss of connectivity. After the upgrade or migration to vCenter Server 6.7 is complete, run the TLS Configurator Utility on each Platform Services Controller node to disable the less secure TLS 1.0 and TLS 1.1 protocols, and use the TLS 1.2 protocol.

For a list of VMware products that support disabling TLS 1.0 and TLS 1.1, see VMware Knowledge Base article 2145796. To learn how to manage TLS protocol configuration, and use the TLS Configurator Utility, see the *VMware Security* documentation.

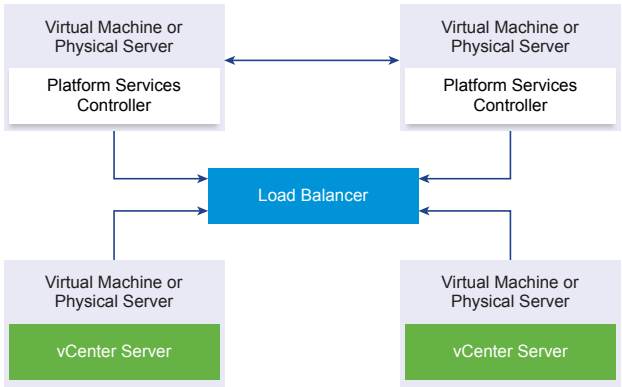
Deployment Topologies with External Platform Services Controller Instances and High Availability

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.

Note vCenter Server deployments using an external Platform Services Controller will not be supported in a future vSphere release. Deploy or upgrade to a vCenter Server deployment using an embedded Platform Services Controller. For more information, see Knowledge Base article KB 60229.

Platform Services Controller with a Load Balancer

Figure 2-9. Example of a Load Balanced Pair of Platform Services Controller Instances



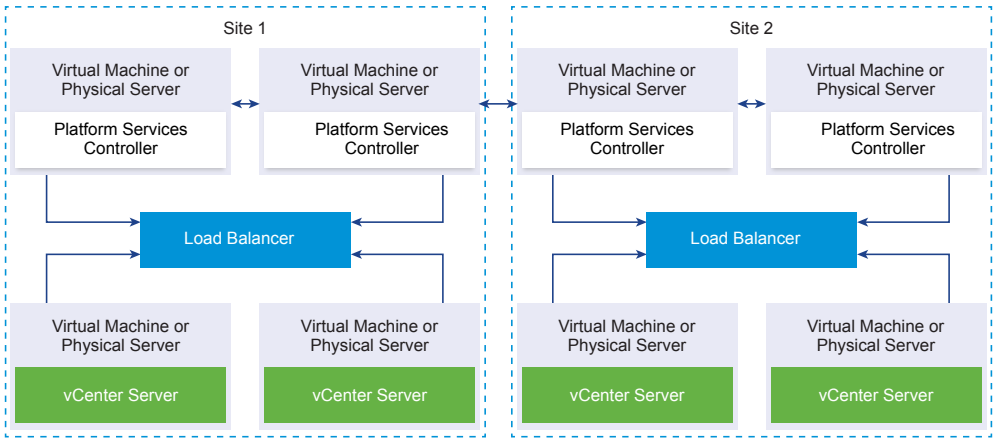
You can use a third-party load balancer per site to configure Platform Services Controller high availability with automatic failover for this site. For information about the maximum number of Platform Services Controller instances behind a load balancer, see the *Configuration Maximums* documentation.

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

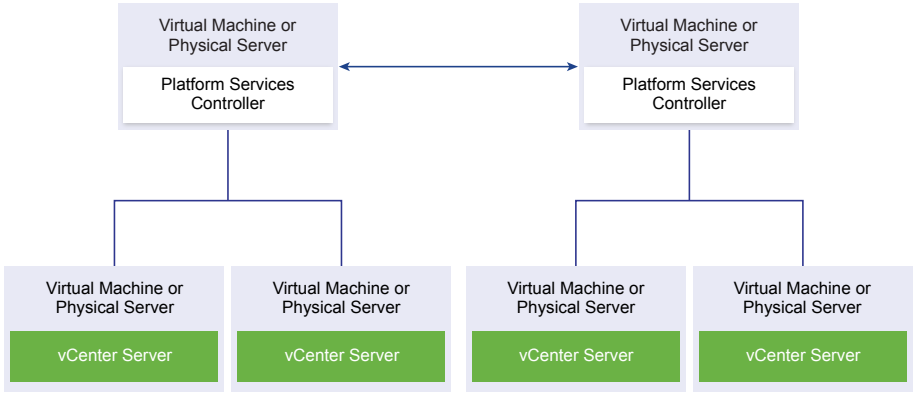
Figure 2-10. Example of Two Load Balanced Pairs of Platform Services Controller Instances Across Two Sites



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 2-11. Example of Two Joined Platform Services Controller Instances with No a Load Balancer

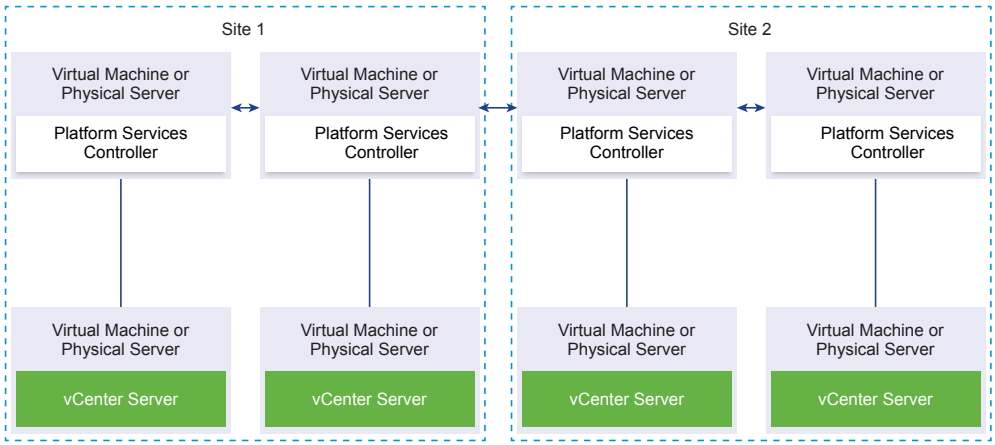


When you join two or more Platform Services Controller instances in the same site with no load balancer, you configure Platform Services Controller high availability with a manual failover for this site.

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 2-12. Example of Two Joined Pairs of Platform Services Controller Instances Across Two Sites with No Load Balancer



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

Before you upgrade or migrate your environment to vSphere 6.7, you must move any deprecated deployment topology to a supported deployment topology.

When you first install vCenter Server 6.0 or 6.5, your deployment includes either an embedded Platform Services Controller or vCenter Single Single-On, or an external Platform Services Controller or vCenter Single Single-On.

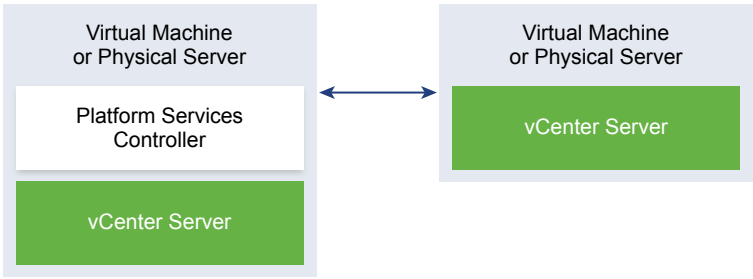
If you upgrade or migrate your deployment later you have two options:

- 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 6.7, you must move any deprecated deployment topology to a supported deployment topology.

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

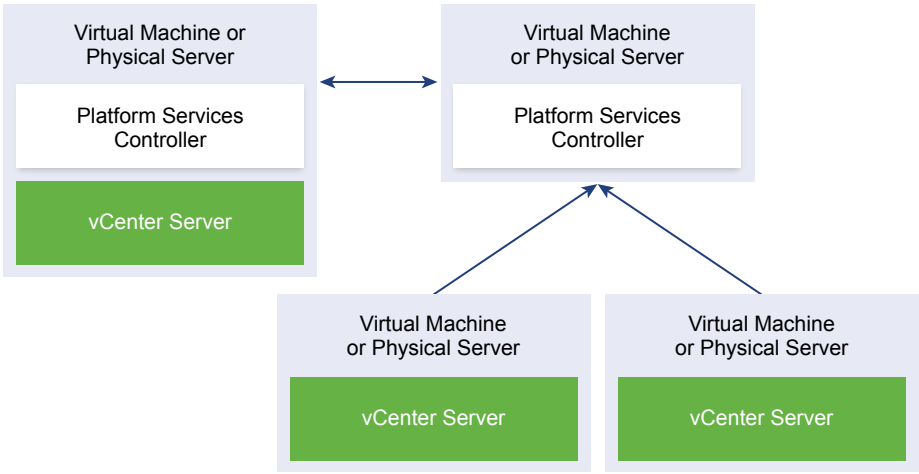
Figure 2-13. Deprecated topology of a vCenter Server Pointing to an Embedded Platform Services Controller



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 2-14. Deprecated Topology of an Embedded Platform Services Controller and an External Platform Services Controller in Replication



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.

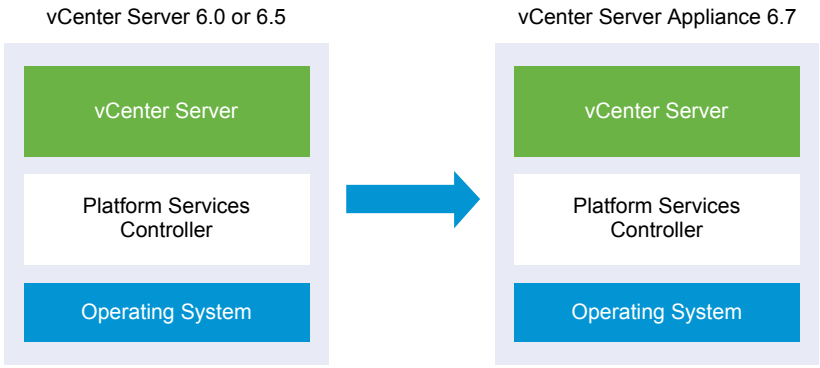
Example Upgrade Paths from vCenter Server version 6.x to version 6.7

Your vCenter Server 6.0.x and 6.5.x deployment type does not change during the upgrade to version 6.7.

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

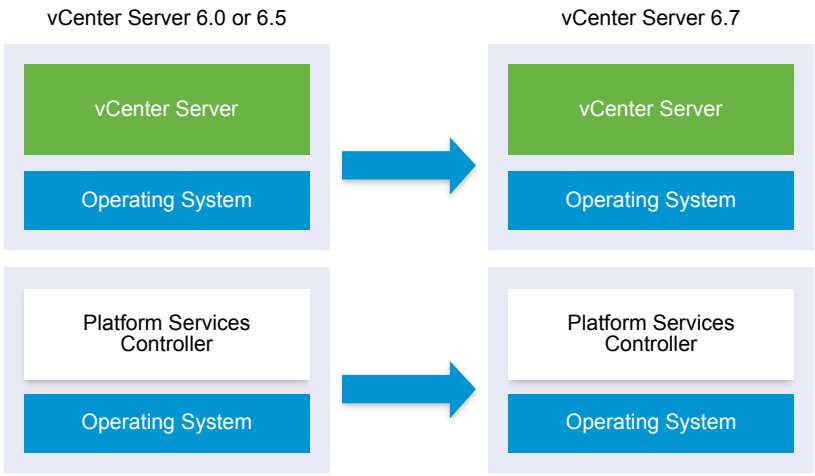
The installer upgrades vCenter Server 6.0 and 6.5 with an embedded Platform Services Controller instance to vCenter Server 6.7 with an embedded Platform Services Controller instance. The software upgrades vCenter Server and Platform Services Controller instance in the correct order to the same version.

Figure 2-15. vCenter Server 6.0.x with Embedded Platform Services Controller Before and After Upgrade



The installer upgrades an external vCenter Server 6.0 and 6.5 instance to an external vCenter Server 6.7 instance and an external Platform Services Controller 6.0 and 6.5 instance to an external Platform Services Controller 6.7 instance.

Figure 2-16. 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 6.7

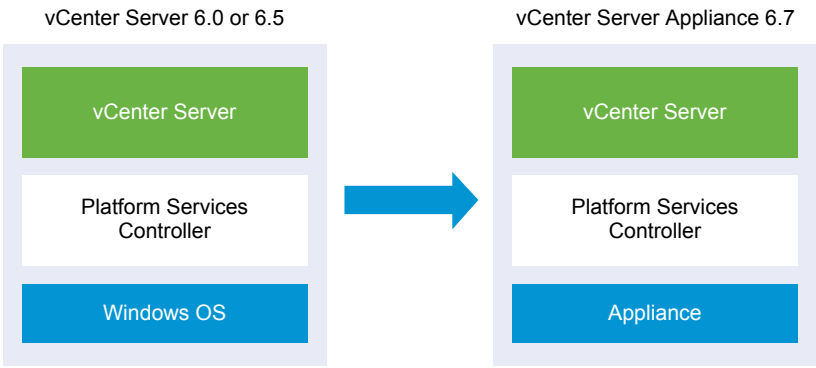
You can migrate a vCenter Server for Windows instance to a vCenter Server Appliance instance.

You can migrate a vCenter Server version 6.0 or 6.5 instance on Windows to a vCenter Server Appliance 6.7 deployment on a Linux-based OS.

The vCenter Server example migration paths demonstrate supported migration outcomes.

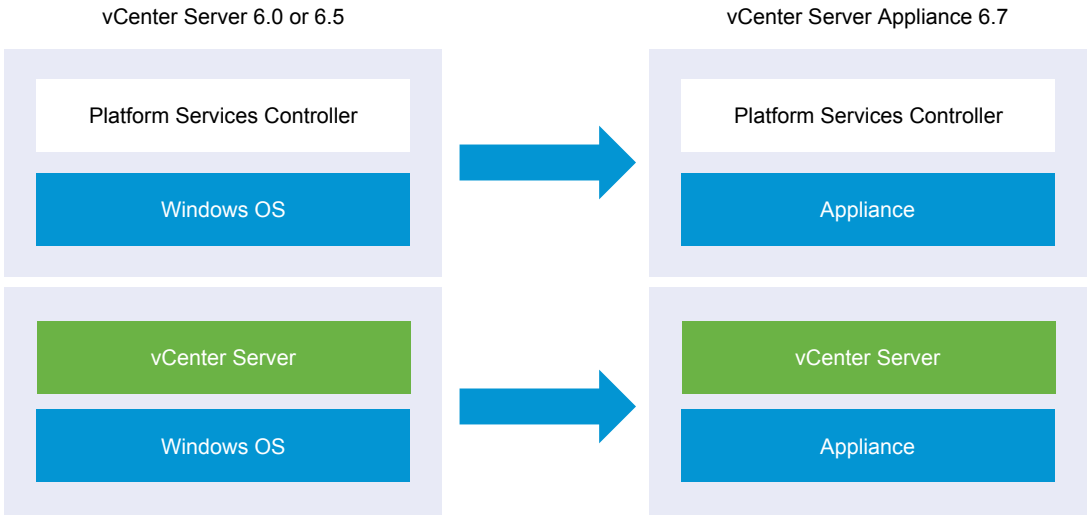
You can migrate a vCenter Server instance with an embedded Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.7 instance with an embedded Platform Services Controller appliance. In this case the software migrates the vCenter Server instance and the embedded Platform Services Controller instance at the same time.

Figure 2-17. vCenter Server 6.x with Embedded Platform Services Controller Installation Before and After Migration



You can migrate a vCenter Server instance with an external Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.7 instance with an external Platform Services Controller appliance. In this case you must first migrate the external Platform Services Controller instance and then the vCenter Server instance.

Figure 2-18. vCenter Server 6.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 vCenter Server for Windows

3

You can upgrade vCenter Server version 6.0 and version 6.5 deployments for Windows to vCenter Server version 6.7 deployments for Windows.

The vCenter Server upgrade includes a database schema upgrade, upgrade of 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 deployment types and versions.

Table 3-1. Supported vSphere Upgrade Paths

Before Upgrade	After Upgrade
vCenter Server 6.0 with an embedded Platform Services Controller on Windows	vCenter Server 6.7 with an embedded Platform Services Controller on Windows
vCenter Server 6.5 with an embedded Platform Services Controller instance on Windows	
Platform Services Controller 6.0 on Windows	Platform Services Controller 6.7 on Windows
Platform Services Controller 6.5 on Windows	
vCenter Server 6.0 on Windows	vCenter Server 6.7 on Windows
vCenter Server 6.5 on Windows	

For upgrade steps for a vCenter Server 6.0 deployment, see Upgrading vCenter Server 6.0 or 6.5 on Windows.

Important You cannot change your deployment type during upgrade.

You cannot uninstall or reinstall individual services during the upgrade process.

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 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 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-Upgrade Checks for vCenter Server and Platform Services Controller on Windows

When you 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 upgrading vCenter Server, and verifies that the external database, if any, can be successfully accessed.

When you upgrade Platform Services Controller (version 6.0) vCenter Single Sign-On is included as part of 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. 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 upgrade 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 upgrade vCenter Server with an embedded Platform Services Controller, you upgrade vCenter Server and the Platform Services Controller on the same virtual machine or physical server. When you upgrade 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 upgrade vCenter Server and the vCenter Server components on another virtual machine or physical server.

Note Upgrading 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 upgrade, you can select a folder other than the default `C:\Program Files\VMware` folder to upgrade vCenter Server and 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 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 Knowledge Base article 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.

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

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a 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.

Note In Microsoft Windows Server 2008 and later, firewall is enabled by default.

Table 3-4. Ports Required for Communication Between Components

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
22	TCP	System port for SSHD. **Important** This port must be open during the upgrade of the appliance. The upgrade process establishes an SSH connection to transfer the data from the existing to the new appliance.	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
53		DNS service	Windows installations and appliance deployments of Platform Services Controller	No

Table 3-4. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
80	TCP	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server. WS-Management (also requires port 443 to be open). If you use a Microsoft SQL database that is stored on the same virtual machine or physical server as the vCenter Server, port 80 is used by the SQL Reporting Service. When you install or upgrade vCenter Server, the installer prompts you to change the HTTP port for vCenter Server. Change the vCenter Server HTTP port to a custom value to ensure a successful installation or upgrade. **Important** You can only change this port number during the vCenter Server and Platform Services Controller installation.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
88	TCP	Active Directory server. This port must be open for host to join Active Directory. If you use native Active Directory, the port must be open on both vCenter Server and Platform Services Controller.	Windows installations and appliance deployments of Platform Services Controller	No
389	TCP/UDP	This port must be open on the local and all remote instances of vCenter Server. This is the LDAP port number for the Directory Services for the vCenter Server group. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the LDAP service on any port from 1025 through 65535. If this instance is serving as the Microsoft Windows Active Directory, change the port number from 389 to an available port from 1025 through 65535.	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to Platform Services Controller

Table 3-4. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
443	TCP	The default port that the vCenter Server system uses to listen for connections from the vSphere Web Client. To enable the vCenter Server system to receive data from the vSphere Web Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. This port is also used for the following services: ■ WS-Management (also requires port 80 to be open) ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts **Important** You only can change this port number during the vCenter Server and Platform Services Controller installation.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	■ vCenter Server to vCenter Server ■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server
514	TCP/UDP	vSphere Syslog Collector port for vCenter Server on Windows and vSphere Syslog Service port for vCenter Server Appliance **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
636	TCP	vCenter Single Sign-On LDAPS For backward compatibility with vSphere 6.0 only.	Windows installations and appliance deployments of Platform Services Controller	During upgrade from vSphere 6.0 only. vCenter Server 6.0 to Platform Services Controller 6.5

Table 3-4. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
902	TCP/UDP	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts. Port 902 must not be blocked between the VMware Host Client and the hosts. The VMware Host Client uses this port to display virtual machine consoles **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
1514	TCP	vSphere Syslog Collector TLS port for vCenter Server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
2012	TCP	Control interface RPC for vCenter Single Sign-On	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server ■ Platform Services Controller to Platform Services Controller
2014	TCP	RPC port for all VMCA (VMware Certificate Authority) APIs **Important** You can change this port number during the Platform Services Controller installations on Windows.	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server
2015	TCP	DNS management	Windows installations and appliance deployments of Platform Services Controller	Platform Services Controller to Platform Services Controller

Table 3-4. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
2020	TCP/UDP	Authentication framework management **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server
5480	TCP	Appliance Management Interface Open endpoint serving all HTTPS, XMLRPS and JSON-RPC requests over HTTPS.	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
6500	TCP/UDP	ESXi Dump Collector port **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
6501	TCP	Auto Deploy service **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
6502	TCP	Auto Deploy management **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
7080, 12721	TCP	Secure Token Service **Note** Internal ports	Windows installations and appliance deployments of Platform Services Controller	No
7081	TCP	VMware Platform Services Controller Web Client **Note** Internal port	Windows installations and appliance deployments of Platform Services Controller	No
7475, 7476	TCP	VMware vSphere Authentication Proxy	Appliance deployments of vCenter Server	Platform Services Controller to vCenter Server
8200, 8201, 8300, 8301	TCP	Appliance management **Note** Internal ports	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No

Table 3-4. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
8084	TCP	vSphere Update Manager SOAP port The port used by vSphere Update Manager client plug-in to connect to the vSphere Update Manager SOAP server.	Appliance deployments of vCenter Server	No
9084	TCP	vSphere Update Manager Web Server Port The HTTP port used by ESXi hosts to access host patch files from vSphere Update Manager server.	Appliance deployments of vCenter Server	No
9087	TCP	vSphere Update Manager Web SSL Port The HTTPS port used by vSphere Update Manager client plug-in to upload host upgrade files to vSphere Update Manager server.	Appliance deployments of vCenter Server	No
9443	TCP	vSphere Web Client HTTPS	Windows installations and appliance deployments of vCenter Server	No

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

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

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 6.7 requires Adobe Flash Player v. 16 to 23. For best performance and the most recent security updates, 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 3-5. Supported Guest Operating Systems and Minimum Browser Versions for the vSphere Web Client

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

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 with vCenter Single Sign-On or Platform Services Controller to provide high availability, you must verify that it is supported and configured correctly before upgrading to vCenter Server 6.7.

- Prepare ESXi Hosts for vCenter Server Upgrade

  Before upgrading to vCenter Server 6.7, 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.

If you have solutions or plug-ins, ensure their compatibility with the vCenter Server version to which you are upgrading. See VMware Product Interoperability Matrices.

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, ESXi 5.1, or ESXi 5.5 hosts to version 6.0 or later.
4. If you have ESXi 5.0, ESXi 5.1, or ESXi 5.5 hosts that you choose not to upgrade, you must remove them from the vCenter Server inventory.
5. Upgrade VMware Host Profiles to version 6.0 or later.

   Host Profiles is a vCenter Server tool for designing and deploying ESX and ESXi hosts. Ensure that you are using Host Profiles version 6.0 or later. See Knowledge Base article KB 52932.

6 Upgrade vSphere Distributed Virtual Switch (DVS) version 6.0 or later.

You must upgrade to DVS version 6.0 or later before upgrading to vCenter Server 6.7. See Knowledge Base article KB 52826.

Note DVS version 6.0 or later supports only Network I/O Control version 3. If you are using an earlier version of Network I/O Control, you must upgrade to Network I/O Control version 3. For more information, see the *vSphere Networking* documentation.

7 Verify that you can upgrade your vCenter Server version using an Embedded Linked Mode topology to vCenter Server 6.7 Update 2.

- Upgrading from vCenter Server 6.0 using an Embedded Linked Mode topology to vCenter Server 6.7 Update 2 is supported.
- Upgrading from vCenter Server 6.5 Update 2 using an Embedded Linked Mode topology to vCenter Server 6.7 Update 2 is supported.

Note vCenter Server deployments using an external Platform Services Controller will not be supported in a future vSphere release. Deploy or upgrade to a vCenter Server deployment using an embedded Platform Services Controller. For more information, see Knowledge Base article KB 60229.

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

Procedure

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

vCenter Server is part of VMware vCloud Suite and VMware vSphere, listed under Datacenter & Cloud Infrastructure.

2 VMware provides a SHA-1 hash, a SHA-256 hash, or an MD5 message digest for software downloads. To confirm file integrity, use a SHA-1, SHA-256, and/or a MD5 utility on your computer to calculate your own hash for files downloaded from the VMware web site.

See the VMware Web site topic Using Cryptographic Hashes at https://www.vmware.com/download/cryptographichashes.html.

3 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 6.0 or 6.5 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 6.0 to vCenter Server 6.7.

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 Make a full backup of the vCenter Server database.

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 finish 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 Knowledge Base article KB 1036331.

To migrate the vCenter Server database from Microsoft SQL Express to Microsoft full SQL Server, see Knowledge Base article KB 1028601.

Important If the vCenter Server service is running under the Microsoft Windows built-in system account, you cannot use Integrate Windows for your authentication method.

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 vCenter Server does not support your database 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.

   If your existing database is Microsoft SQL Server, you do not need to install a new vCenter Server instance.

   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 physical vCenter Server machine.
7. Verify that the `sqljdbc4.jar` file is added to the CLASSPATH variable on the physical 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 Make a full backup of the vCenter Server database.

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.

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 3-6. 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 3-6. 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 3-7. Oracle Database Permissions for vCenter Server

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

Table 3-7. Oracle Database Permissions for vCenter Server (Continued)

Permission	Description
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.

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, 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 6.7.
- 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.

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 with vCenter Single Sign-On or Platform Services Controller to provide high availability, you must verify that it is supported and configured correctly before upgrading to vCenter Server 6.7.

In environments with less than four vCenter Server systems, use 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*.

To learn about the use of qualified load balancers that supply high availability, and their requirements between versions of vSphere for use with vCenter Single Sign-On and Platform Services Controller, see Knowledge Base article KB 2112736.

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 6.7, you must prepare your ESXi hosts.

Prerequisites

To upgrade vCenter Server, your ESXi hosts must be at version 6.0. If your ESXi hosts are earlier than 6.0, upgrade them to 6.0. Read and follow all best practices when upgrading your hosts to ESXi 6.0.

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 6.7.

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 Click the **Configure** tab, then click **General** tab.

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

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.

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.

   When upgrading from vCenter Server 6.0 or 6.5, the software preserves your current deployment during the upgrade to vCenter Server 6.7.

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 upgrade a vSphere product, synchronize the clocks of all machines on the vSphere network.

5 If you do not intend to use vCenter Server 6.7 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 6.7.

   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.

Your vCenter Server environment is ready for the upgrade. See Upgrading vCenter Server 6.0 or 6.5 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 physical machines in your vSphere network are not synchronized, SSL certificates and SAML Tokens, 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 `vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause firstboot to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server Appliance is not synchronized with NTP. Similarly, issues can arise if the destination vCenter Server Appliance migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server Appliance.

- The target ESXi host where the destination vCenter Server Appliance is to be deployed is synchronized to NTP.
- The ESXi host running the source vCenter Server Appliance is synchronized to NTP.
- When upgrading or migrating, if the vCenter Server Appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP.
- If you are upgrading or migrating, verify that the source vCenter Server or vCenter Server Appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See Knowledge Base article 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*.

To learn how to change time synchronization settings for vCenter Server Appliance, see "Configuring Time Synchronization Settings in the vCenter Server Appliance" in *vCenter Server Appliance Configuration*.

To learn how to edit time configuration for a host, see "Edit Time Configuration for a Host" in *vCenter Server and 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 6.0 and later to vCenter Server 6.7. To upgrade from vCenter Server 5.0, 5.1 or 5.5, you must first upgrade the vCenter Server instance to version 6.0 or later releases, and then upgrade it to vCenter Server 6.7. For information about upgrading vCenter Server 5.0, 5.1, or 5.5 to version 6.0 or 6.5, see the *VMware vSphere 5.5 Documentation* or *VMware vSphere 6.5 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 3-8. 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			
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 old 5.x data	`C:\ProgramData\VMware\VMware\vCenter Server\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 6.0 or 6.5 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 6.7. For upgrade steps, see Upgrade vCenter Platform Services Controller 6.0 or 6.5 on Windows.

2 Next you upgrade the vCenter Server instance to version 6.7. For upgrade steps, see Upgrade vCenter Server 6.0 or 6.5 on Windows.

Figure 3-1. vCenter Server 6.0 or 6.5 with Embedded Platform Services Controller Deployment Before and After Ugrade

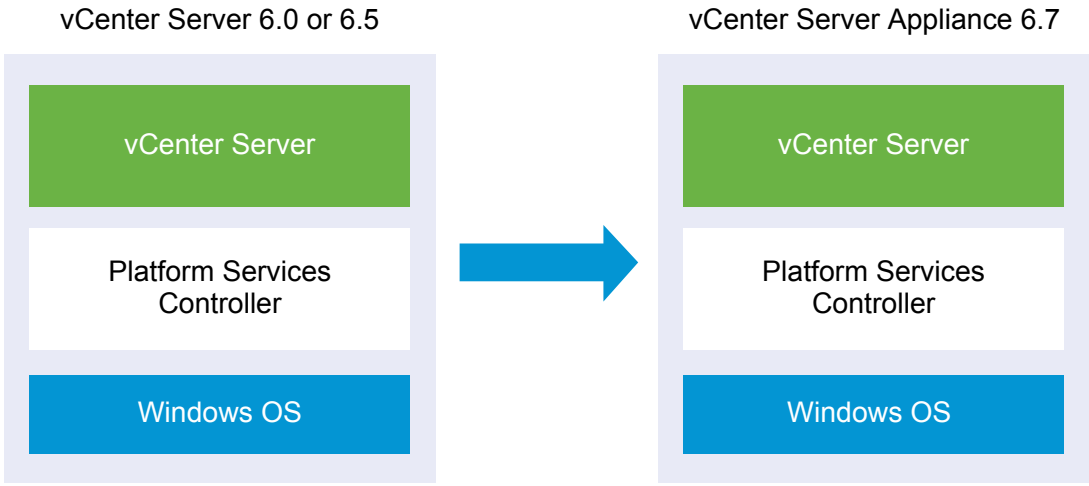
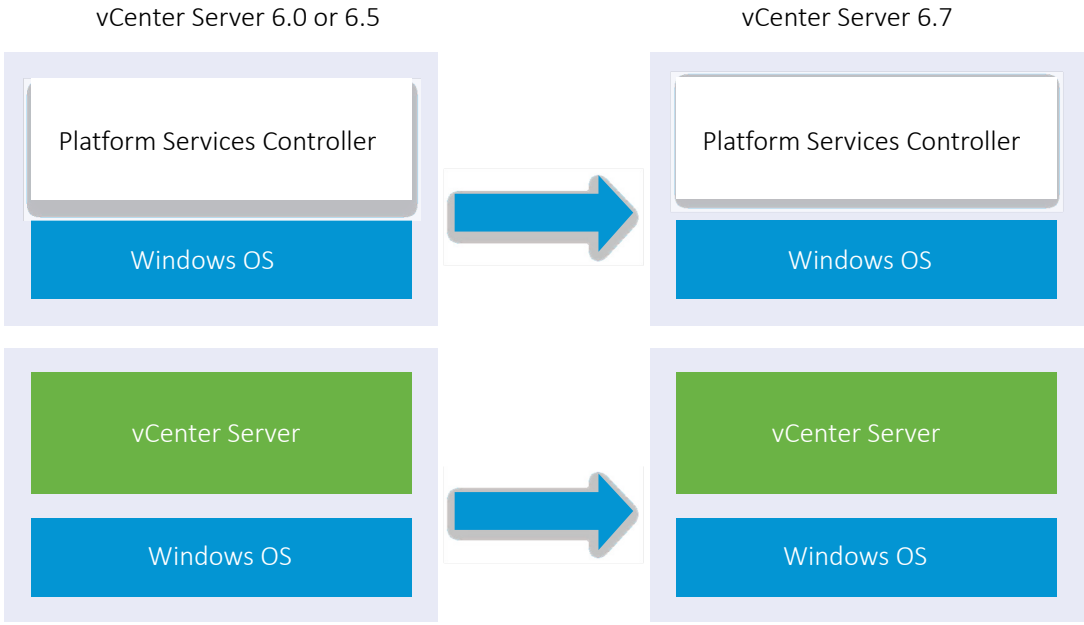


Figure 3-2. vCenter Server 6.0 or 6.5 with External Platform Services Controller Before and After Upgrade



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

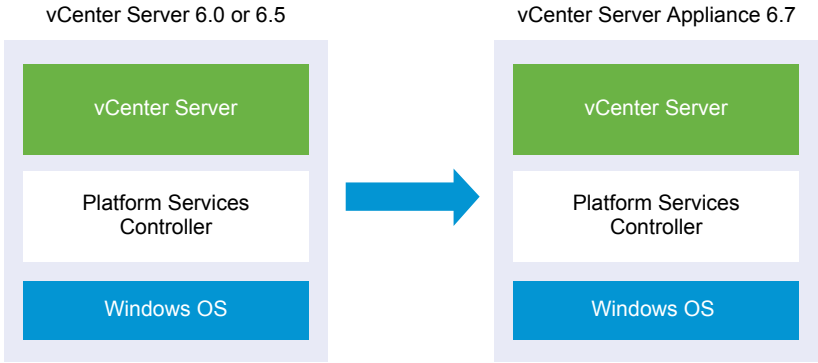
When upgrading vCenter Server instances on Windows in a mixed platform environment with a Platform Services Controller 6.0 or 6.5 appliance, you upgrade the Platform Services Controller appliance to version 6.7 before upgrading the vCenter Server instances. For Platform Services Controller 6.0 appliance 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 6.7. For vCenter Server Appliance 6.0 or 6.5 upgrade steps, see Upgrade a vCenter Server Appliance 6.0 or 6.5 with an External vCenter Single Sign-On or Platform Services Controller Instance by Using the GUI.

Upgrade a vCenter Server 6.0 or 6.5 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 3-3. vCenter Server 6.0 or 6.5 with Embedded Platform Services Controller Deployment Before and After Upgrade



- vCenter Server 6.0 and 6.5 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**.

   The ports in use by vCenter Server and Platform Services Controller are preserved during upgrade.
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.

Your vCenter Server for Windows upgrade is complete.

What to do next

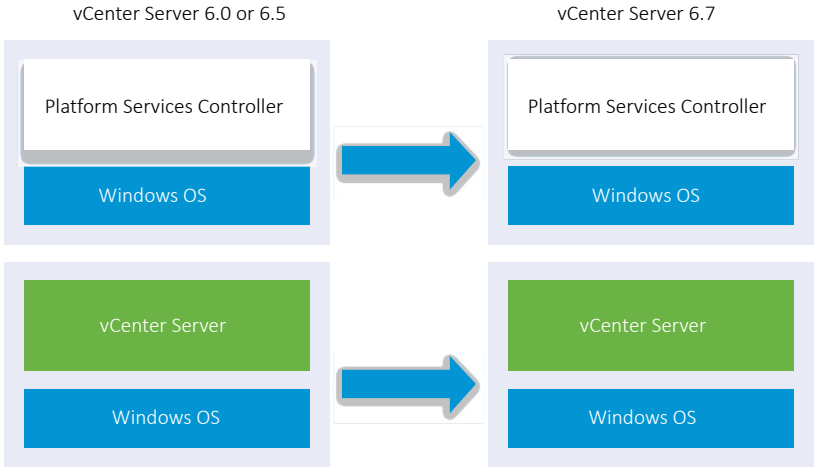
Verify that your upgrade was successful. For verification steps, see Verify Your vCenter Server Appliance Upgrade or Migration Is Successful.

For information on post-upgrade steps, see Chapter 6 After Upgrading or Migrating vCenter Server.

Upgrade vCenter Platform Services Controller 6.0 or 6.5 on Windows

You can upgrade your externally deployed Platform Services Controller 6.0 instance to an externally deployed Platform Services Controller 6.7 instance by using the vCenter Server for Windows installer.

Figure 3-4. vCenter Server 6.0.x with External Platform Services Controller Before and After Upgrade



In a mixed version environment, any vCenter Server 6.0 or 6.5 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 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**.

   The ports in use by vCenter Server and Platform Services Controller are preserved during upgrade.
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 6.7, you can upgrade your vCenter Server instances. For information on upgrading vCenter Server instances on Windows, see Upgrade vCenter Server 6.0 or 6.5 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.

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 or 6.5 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 or 6.5 on Windows

You can upgrade your vCenter Server 6.0 or 6.5 instance to version 6.7 by using the vCenter Server for Windows installer.

The upgrade process preserves your vCenter Server 6.0 or 6.5 configuration.

- If your Platform Services Controller is embedded, the installer upgrades it as part of the vCenter Server upgrade.
- vCenter Server 6.0 or 6.5 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.

- vCenter Server appliance 6.5 and 6.7 support only the embedded PostgreSQL database. If you are migrating from avCenter Server 6.0 deployment using an external Oracle database, the upgrade installer automatically migrates the database from the Oracle database to the embedded PostgreSQL database included with vCenter Server.

Note If you are using any external Platform Services Controller instances, you must upgrade them to Platform Services Controller 6.7 instances before upgrading your vCenter Server 6.0 or 6.5 instances to 6.7.

- 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 or 6.5 on Windows.
- For information on post-upgrade steps, see Chapter 6 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**.

The ports in use by vCenter Server and Platform Services Controller are preserved during upgrade.

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.

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

Upgrading the vCenter Server Appliance and Platform Services Controller Appliance

4

You can upgrade the vCenter Server Appliance 6.0 or 6.5 and the Platform Services Controller appliance 6.0 to version 6.7. All 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 6.7. You can deploy the new appliance on an ESXi host 6.0 or later, or on the inventory of a vCenter Server instance 6.0 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 6.7. At the end of the upgrade, the temporary IP address is released and the old appliance is powered off.

Version 6.7 of the vCenter Server Appliance uses the embedded PostgreSQL database. If you are upgrading a vCenter Server Appliance that uses an external database, the external database is 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 6.7 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 is 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 6.7, see *vCenter Server 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 GUI and CLI upgrade files which you can use alternatively.

Note vCenter Server deployments using an external Platform Services Controller will not be supported in a future vSphere release. Deploy or upgrade to a vCenter Server deployment using an embedded Platform Services Controller. For more information, see Knowledge Base article KB 60229.

- 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 deploys the new appliance. The OVF Tool command also transfers services and configuration data and from the old appliance to the new 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 you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not shown. After the upgrade, you can manually connect the appliance to the original non-ephemeral distributed virtual port group. This is not a limitation when deploying the appliance through a vCenter Server, and you can deploy to ephemeral or non-ephemeral distributed virtual port groups.

To upgrade vCenter Server Appliance version 5.5 or earlier, you must first upgrade to version 6.0 or 6.5 and then upgrade to version 6.7. For information about upgrading vCenter Server Appliance 5.5 to version 6.5, see the *VMware vSphere 6.5* documentation. For information on the upgrade compatibility of vCenter Server, see the VMware Compatibility Guide.

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

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

This chapter includes the following topics:

- GUI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance
- Upgrading vCenter and Platform Services Controller High Availability Environments
- 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 6.0 or 6.5 to version 6.7. You can upgrade the Platform Services Controller appliance from version 6.0 or 6.5 to version 6.7.

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

1 Deploying a new appliance of version 6.7 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 6.0 or 6.5 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

   If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and will not be shown. After the upgrade, you can manually connect the appliance to the original non-ephemeral distributed virtual port group. This is not a limitation when deploying the appliance through a vCenter Server, and you can deploy to ephemeral or non-ephemeral distributed virtual port groups.

   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.

Important If your current vCenter Server Appliance version is version 5.5 or earlier, you must upgrade to version 6.0 or 6.5 before upgrading to version 6.7

Figure 4-1. Upgrade Workflow for a vCenter Server Appliance with an External Platform Services Controller

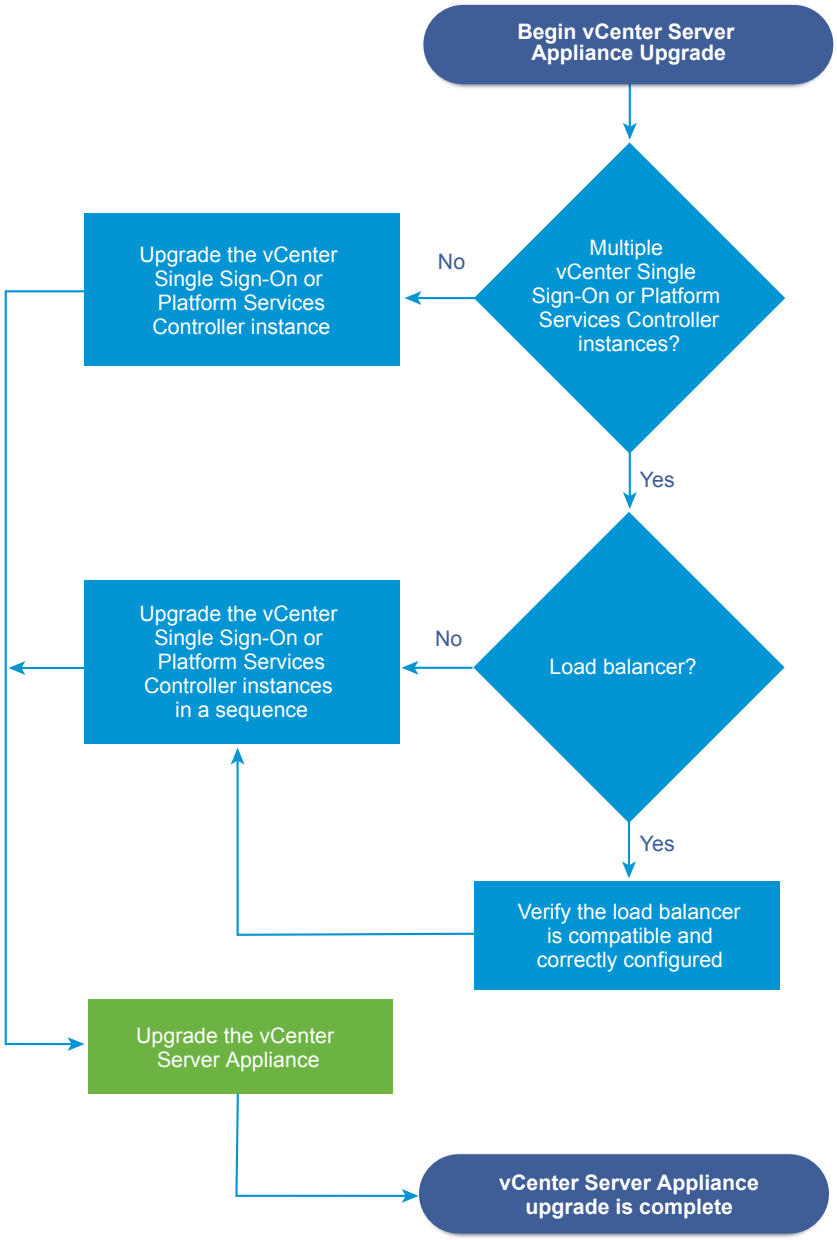


Figure 4-1 states that you must upgrade your Platform Services Controller deployment in sequence. The sequence by which you upgrade Platform Services Controller refers to upgrading the primary, secondary, and any additional Platform Services Controller High Availability (HA) nodes in a specific order. To learn more about the sequence by which you upgrade Platform Services Controller HA deployments, see Upgrade a Platform Services Controller High Availability Appliance 6.0 by Using the GUI.

- 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 4 Upgrading the vCenter Server Appliance and Platform Services Controller Appliance.
- For the appliance post-upgrade procedures, see Chapter 6 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 6.7. You can deploy the new vCenter Server Appliance or Platform Services Controller appliance on an ESXi host 6.0 or later, or on a vCenter Server instance 6.0 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 4-1. 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 4-1. 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 an external 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 4-2. 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)	300 GB	825 GB	1700 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	340 GB	870 GB	1750 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	525 GB	1025 GB	1905 GB

Table 4-2. 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)	740 GB	1090 GB	1970 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	1180 GB	1230 GB	2110 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 an external 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 6.0 hosts or later, or on vCenter Server instances 6.0 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 6.x host on which to deploy the appliance. You can also connect to a vCenter Server 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.

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

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a 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.

Note In Microsoft Windows Server 2008 and later, firewall is enabled by default.

Table 4-3. Ports Required for Communication Between Components

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
22	TCP	System port for SSHD. **Important** This port must be open during the upgrade of the appliance. The upgrade process establishes an SSH connection to transfer the data from the existing to the new appliance.	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
53		DNS service	Windows installations and appliance deployments of Platform Services Controller	No
80	TCP	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server. WS-Management (also requires port 443 to be open). If you use a Microsoft SQL database that is stored on the same virtual machine or physical server as the vCenter Server, port 80 is used by the SQL Reporting Service. When you install or upgrade vCenter Server, the installer prompts you to change the HTTP port for vCenter Server. Change the vCenter Server HTTP port to a custom value to ensure a successful installation or upgrade. **Important** You can only change this port number during the vCenter Server and Platform Services Controller installation.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No

Table 4-3. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
88	TCP	Active Directory server. This port must be open for host to join Active Directory. If you use native Active Directory, the port must be open on both vCenter Server and Platform Services Controller.	Windows installations and appliance deployments of Platform Services Controller	No
389	TCP/UDP	This port must be open on the local and all remote instances of vCenter Server. This is the LDAP port number for the Directory Services for the vCenter Server group. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the LDAP service on any port from 1025 through 65535. If this instance is serving as the Microsoft Windows Active Directory, change the port number from 389 to an available port from 1025 through 65535.	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to Platform Services Controller
443	TCP	The default port that the vCenter Server system uses to listen for connections from the vSphere Web Client. To enable the vCenter Server system to receive data from the vSphere Web Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. This port is also used for the following services: ■ WS-Management (also requires port 80 to be open) ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts **Important** You only can change this port number during the vCenter Server and Platform Services Controller installation.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	■ vCenter Server to vCenter Server ■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server

Table 4-3. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
514	TCP/UDP	vSphere Syslog Collector port for vCenter Server on Windows and vSphere Syslog Service port for vCenter Server Appliance **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
636	TCP	vCenter Single Sign-On LDAPS For backward compatibility with vSphere 6.0 only.	Windows installations and appliance deployments of Platform Services Controller	During upgrade from vSphere 6.0 only. vCenter Server 6.0 to Platform Services Controller 6.5
902	TCP/UDP	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts. Port 902 must not be blocked between the VMware Host Client and the hosts. The VMware Host Client uses this port to display virtual machine consoles **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
1514	TCP	vSphere Syslog Collector TLS port for vCenter Server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	No

Table 4-3. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
2012	TCP	Control interface RPC for vCenter Single Sign-On	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server ■ Platform Services Controller to Platform Services Controller
2014	TCP	RPC port for all VMCA (VMware Certificate Authority) APIs **Important** You can change this port number during the Platform Services Controller installations on Windows.	Windows installations and appliance deployments of Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server
2015	TCP	DNS management	Windows installations and appliance deployments of Platform Services Controller	Platform Services Controller to Platform Services Controller
2020	TCP/UDP	Authentication framework management **Important** You can change this port number during the vCenter Server and Platform Services Controller installations on Windows.	Windows installations and appliance deployments of ■ vCenter Server ■ Platform Services Controller	■ vCenter Server to Platform Services Controller ■ Platform Services Controller to vCenter Server
5480	TCP	Appliance Management Interface Open endpoint serving all HTTPS, XMLRPS and JSON-RPC requests over HTTPS.	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
6500	TCP/UDP	ESXi Dump Collector port **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
6501	TCP	Auto Deploy service **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No

Table 4-3. Ports Required for Communication Between Components (Continued)

Port	Protocol	Description	Required for	Used for Node-to-Node Communication
6502	TCP	Auto Deploy management **Important** You can change this port number during the vCenter Server installations on Windows.	Windows installations and appliance deployments of vCenter Server	No
7080, 12721	TCP	Secure Token Service **Note** Internal ports	Windows installations and appliance deployments of Platform Services Controller	No
7081	TCP	VMware Platform Services Controller Web Client **Note** Internal port	Windows installations and appliance deployments of Platform Services Controller	No
7475, 7476	TCP	VMware vSphere Authentication Proxy	Appliance deployments of vCenter Server	Platform Services Controller to vCenter Server
8200, 8201, 8300, 8301	TCP	Appliance management **Note** Internal ports	Appliance deployments of ■ vCenter Server ■ Platform Services Controller	No
8084	TCP	vSphere Update Manager SOAP port The port used by vSphere Update Manager client plug-in to connect to the vSphere Update Manager SOAP server.	Appliance deployments of vCenter Server	No
9084	TCP	vSphere Update Manager Web Server Port The HTTP port used by ESXi hosts to access host patch files from vSphere Update Manager server.	Appliance deployments of vCenter Server	No
9087	TCP	vSphere Update Manager Web SSL Port The HTTPS port used by vSphere Update Manager client plug-in to upload host upgrade files to vSphere Update Manager server.	Appliance deployments of vCenter Server	No
9443	TCP	vSphere Web Client HTTPS	Windows installations and appliance deployments of vCenter Server	No

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

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

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 Client Software Requirements

Use of the vSphere Client requires a supported Web browser.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Client.

Table 4-4. Supported Guest Operating Systems and Browser Versions for the vSphere Client .

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Internet Explorer 11 and later. Mozilla Firefox: 56 and later. Google Chrome: 62 and later.
Mac OS	Mozilla Firefox: 56 and later. Google Chrome: 62 and later.

Later versions of these browsers are likely to work, but have not been tested.

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 4-5. 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.

Note Visual C++ redistributable libraries need to be installed to run the CLI installer on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa-cli-installer/win32/vcredist` directory.

Note Deploying the vCenter Server Appliance with the GUI requires a minimum resolution of 1024x768 to properly display. Lower resolutions can truncate the UI elements.

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 My VMware 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 From the VMware Web site at https://my.vmware.com/web/vmware/downloads, download the vCenter Server Appliance ISO image.

`VMware-VCSA-all-version_number-build_number.iso`

2 Confirm that the md5sum is correct.

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

3 Mount 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, for example, MagicISO Maker on Windows, is unsupported.

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 physical machines in your vSphere network are not synchronized, SSL certificates and SAML Tokens, 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 `vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause firstboot to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server Appliance is not synchronized with NTP. Similarly, issues can arise if the destination vCenter Server Appliance migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server Appliance.

- The target ESXi host where the destination vCenter Server Appliance is to be deployed is synchronized to NTP.
- The ESXi host running the source vCenter Server Appliance is synchronized to NTP.
- When upgrading or migrating, if the vCenter Server Appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP.
- If you are upgrading or migrating, verify that the source vCenter Server or vCenter Server Appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See Knowledge Base article 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*.

To learn how to change time synchronization settings for vCenter Server Appliance, see "Configuring Time Synchronization Settings in the vCenter Server Appliance" in *vCenter Server Appliance Configuration*.

To learn how to edit time configuration for a host, see "Edit Time Configuration for a Host" in *vCenter Server and Host Management*.

Transferring Data from an Existing vCenter Server Appliance

You can transfer data from an existing vCenter Server Appliance external database to the embedded PostgreSQL database in use by version 6.7 of the vCenter Server Appliance.

Both the Windows-based vCenter Server upgrade and vCenter Server Appliance migration procedures let you copy the minimum amount of data needed to be operational, minimizing downtime. You can then copy the remaining data from the external database to the embedded PostgreSQL database in the background, preserving your deployment's historical event and performance data.

You can migrate the following types of data from an external database to the embedded PostgreSQL database in use by version 6.7 of the vCenter Server Appliance.

Configuration data

This is the minimum type of data you must transfer from your existing vCenter Server Appliance external database to upgrade or migrate to a functioning vCenter Server Appliance. This data can be transferred in a reasonably short amount of time, minimizing downtime during the upgrade to vCenter Server Appliance 6.7.

Configuration and historical data

In addition to the configuration data, you can choose to transfer historical data such as usage statistics, events, and tasks. The vCenter Server Appliance installer gives you the option to copy both the configuration and historical data at once, or to copy only the configuration data during the upgrade process. You can then choose to copy the historical data in the background after you start your new vCenter Server.

Attention If you choose to copy all data and once, you cannot start vCenter Server until all of the data has been transferred to the embedded PostgreSQL database within vCenter Server Appliance 6.7.

Configuration, historical, and performance metrics data

This is the largest amount of data you can choose to transfer to vCenter Server Appliance. As with the configuration and historical data, you can choose to copy only the configuration data during the upgrade process, and then copy the historical and performance data in the background after the upgrade or migration to vCenter Server Appliance 6.7 is complete.

You can transfer historical data after the upgrade or migration from the following vCenter Server versions and external databases to the embedded PostgreSQL database within vCenter Server Appliance.

Table 4-6. vCenter Server database support for data transfer after upgrade or migration

vCenter Server Versions	Databases	vCenter Server Appliance 6.7 Support for Data Transfer
vCenter Server Appliance 6.0	External Oracle database	Supported
	Embedded PostgreSQL database	Not supported
vCenter Server for Windows 6.0	External Oracle or MS SQL database	Supported
	Embedded PostgreSQL database	Not supported
vCenter Server Appliance 6.5	Embedded PostgreSQL database	Not supported
vCenter Server for Windows 6.5	External Oracle or MS SQL database	Supported
	Embedded PostgreSQL database	Not supported

Monitor and Manage Historical Data Migration

You can monitor and mange the background migration of historical data using the vCenter Server Appliance Management Interface. You can perform the following data management tasks:

- Monitor the progress of the data migration.
- Pause the data import.
- Cancel the data import.

> **Important** If you cancel the data import, the historical data will not be imported to the embedded PostgreSQL database. You cannot recover the data once you cancel the operation. If you do cancel the import, and wish to import the historical data at a later time, you must restart the upgrade or migration process from Stage 1 of the GUI installer.

See Monitor and Manage Historical Data Migration.

Prepare ESXi Hosts for vCenter Server Appliance Upgrade

Before upgrading to vCenter Server Appliance 6.7, 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 6.0 or later. Read and follow all best practices when upgrading your hosts to ESXi 6.0 or later. For information on ESXi compatibility, see the VMware Compatibility Guide.
- Your source and target ESXi hosts must not be in lockdown or maintenance mode, and not part of fully automated DRS clusters.
- Review your environment's Certificate Authority (CA) signed SSL certificates. To learn about manually reviewing CA signed SSL certificates in a vSphere environment, see Knowledge Base article KB 2111411.

Procedure

1. If you have Custom or Thumbprint certificates, see Host Upgrades and Certificates to determine your preparatory steps.
2. 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 **Configure** tab, and then under **Settings** select **General**.

   c. Click **Edit**.

   d. Select **SSL settings**.

   Verify that **vCenter Server requires verified host SSL certificates** is selected.

Your ESXi hosts are ready for the 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.

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 that is managed by vCenter Server, review the DRS settings on the cluster. Ensure that the DRS settings for the cluster on which the target ESXi host resides are not configured for Full Automation.

  VMware recommends setting the Automation Level to Manual or Partially Automated. This ensures that the target ESXi host does not reboot during the upgrade process.
- 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

- Ensure that DRS is set to manual for the cluster temporarily so that the VMs for the Source and Target do not get moved during the upgrade.
- 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 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.
- 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 a snapshot of the appliance you want to upgrade as a precaution in case of failure during the upgrade process. If you are upgrading a vCenter Server Appliance with an external Platform Services Controller, take a snapshot of the Platform Services Controller appliance as well.
- 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 4-2. 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 6.0 or later, 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 4-3. 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 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5

The GUI upgrade wizard prompts you for information about the vCenter Server Appliance or Platform Services Controller appliance that you want to upgrade, deployment information for the new 6.7 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 6.0 or 6.5 with an embedded Platform Services Controller, a vCenter Server Appliance 6.0 or 6.5 with an external Platform Services Controller, or a Platform Services Controller appliance 6.0 or 6.5.

Table 4-7. 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	
	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	-	

Table 4-7. Required Information During Stage 1 of the Upgrade (Continued)

Required for Upgrade of	Required Information	Default	Your Entry
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.	-	
	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 .	-	

Table 4-7. Required Information During Stage 1 of the Upgrade (Continued)

Required for Upgrade of	Required Information	Default	Your Entry
All deployment types	The virtual machine 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 the lower ASCII character set 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 4-7. Required Information During Stage 1 of the Upgrade (Continued)

Required for Upgrade of	Required Information	Default	Your Entry
■ vCenter Server Appliance 6.0 with an embedded Platform Services Controller ■ vCenter Server Appliance 6.0 with an external Platform Services Controller ■ vCenter Server Appliance 6.5 with an embedded Platform Services Controller ■ vCenter Server Appliance 6.5 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.	The size of the source vCenter Server Appliance and Platform Services Controller determines the default deployment size. Using this information, the upgrade installer calculates the best size to use for your environment, which might be the same as your existing deployment, or calculated to the next largest size.	

Table 4-7. Required Information During Stage 1 of the Upgrade (Continued)

Required for Upgrade of	Required Information	Default	Your Entry
■ vCenter Server Appliance 6.0 with an external Platform Services Controller ■ vCenter Server Appliance 6.5 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 **Note** The sizing algorithm in use by the upgrade installer might select a larger storage size for your environment. Items that might affect the storage size selected by the installer include modifications to the vCenter Server Appliance disks (for example, changing the size of the logging partition), or databases having a database table that the installer determines to be exceptionally large and requiring additional hard disk space.	

Table 4-7. 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 physical 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 4-7. 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 a DHCP assignment with IPv4 version for the temporary IP address and a DDNS server is available in your environment.	Temporary system name (FQDN).	-	

Table 4-8. Required Information During Stage 2 of the Upgrade

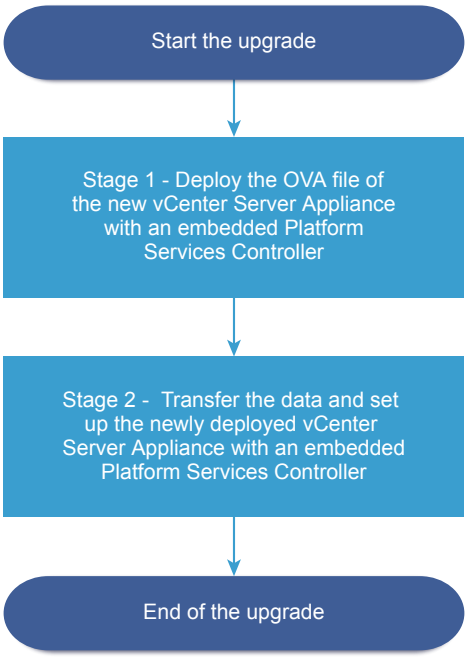
Required for	Required Information	Default	Your Entry
■ vCenter Server Appliance 6.0 with an embedded or external Platform Services Controller ■ vCenter Server Appliance 6.5 with an embedded or external Platform Services Controller	Data types to transfer from the old appliance to the new appliance. In 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 6.0 with an embedded Platform Services Controller ■ Platform Services Controller 6.0 appliance ■ vCenter Server Appliance 6.5 with an embedded Platform Services Controller ■ Platform Services Controller 6.5 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 6.0 or 6.5 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 6.0 or 6.5 that uses an embedded vCenter Single Sign-On or Platform Services Controller to vCenter Server Appliance 6.7 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 6.7of the vCenter Server Appliance and Platform Services Controller appliance on hosts that are running ESXi 6.0 or later and on vCenter Server instances 6.0 or later.

Figure 4-4. 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 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.

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 6.7 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	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with vCenter Server Appliance version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

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 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**.

8 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.

9 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

10 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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 GB of storage.

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**. NFS datastores are thin provisioned by default.

12 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.

13 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.

14 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.

The newly deployed vCenter Server Appliance 6.7 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 6.7 with an embedded Platform Services Controller.

Prerequisites

Understand the data migration options available to you when upgrading or migrating to a vCenter Server Appliance with an embedded PostgreSQL database. You can choose to migrate historical and other types of data in the background after deploying and starting vCenter Server Appliance. See Transferring Data from an Existing vCenter Server Appliance.

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 migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server Appliance.

4. 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*.

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

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

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

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

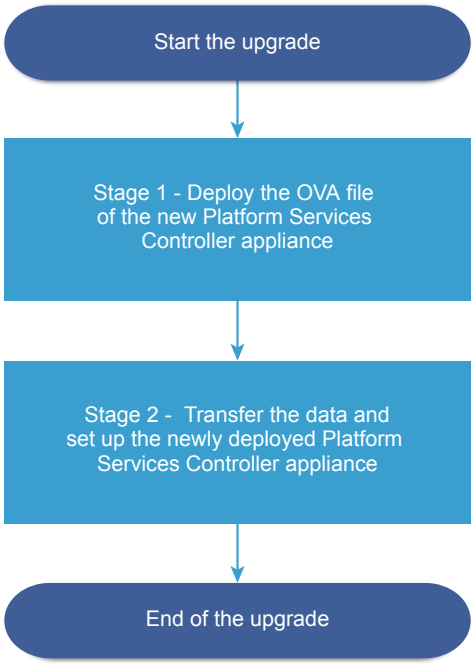
You can use the GUI installer to perform an interactive upgrade of a Platform Services Controller appliance 6.0 to version 6.7. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

Important You must upgrade Platform Services Controller instances configured for High Availability (HA) in an ordered sequence.

When upgrading multiple instances of Platform Services Controllerconfigured in a HA environment, you upgrade the instances one by one in sequence. To learn about upgrading Platform Services Controller in sequence, see Knowledge Base article KB 53661.

Note vCenter Server deployments using an external Platform Services Controller will not be supported in future a vSphere release. Deploy or upgrade to a vCenter Server deployment using an embedded Platform Services Controller. For more information, see Knowledge Base article KB 60229.

Figure 4-5. 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 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.

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 6.7.

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 6.7.

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 6.7.

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	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with Platform Services Controller version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

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**. NFS datastores are thin provisioned by default.

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.

The newly deployed Platform Services Controller appliance 6.7 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 6.7.

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.

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

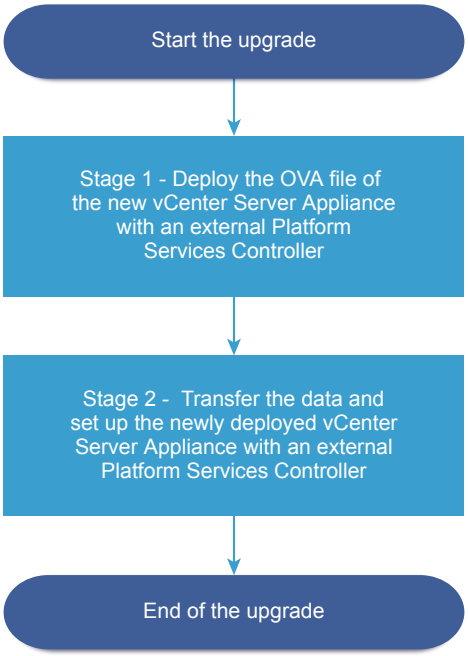
What to do next

- When the upgrade finishes, you must run the scripts `updateSSOConfig.py` and `UpdateLsEndpoint.py` to configure the Platform Services Controller HA nodes for load balancing. For more information, see Knowledge Base article KB 53664.
- To learn about configuring load balancers for use in a Platform Services Controller HA environment, see Knowledge Base article KB 53661.
- 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 6.0 or 6.5 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 6.0 or 6.5 that uses an external vCenter Single Sign-On or Platform Services Controller instance to vCenter Server Appliance 6.7 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 4-6. 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 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.
- Upgrade or migrate the external Platform Services Controller 6.0 instances in the domain to Platform Services Controller 6.7.

Procedure

1 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 6.7 with an external Platform Services Controller.

2 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 6.7 with an external Platform Services Controller.

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 6.7 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	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with vCenter Server Appliance version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

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 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**.

8 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.

9 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

10 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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 GB of storage.

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**. NFS datastores are thin provisioned by default.

12 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.

13 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.

14 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.

The newly deployed target vCenter Server Appliance 6.7 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 6.7 with an external Platform Services Controller.

Prerequisites

Understand the data migration options available to you when upgrading or migrating to a vCenter Server Appliance with an embedded PostgreSQL database. You can choose to migrate historical and other types of data in the background after deploying and starting vCenter Server Appliance. See Transferring Data from an Existing vCenter Server Appliance.

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 migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server Appliance.

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.

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*.

Upgrading vCenter and Platform Services Controller High Availability Environments

You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance or Platform Services Controller in a high availability (HA) environment.

- Prerequisites for Upgrading vCenter Server High Availability Environments

  To ensure a successful upgrade of vCenter Server or Platform Services Controller in a high availability (HA) environment, your environment must meet certain prerequisites before running the upgrade.

- Upgrade a vCenter Server Appliance 6.5 HA Cluster with an Embedded vCenter Platform Services Controller by Using the GUI

  You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance 6.5 in a High Availability (HA) cluster that uses an embedded vCenter Single Sign-On or Platform Services Controller to vCenter Server Appliance 6.7 with an embedded Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

- Upgrade a Platform Services Controller High Availability Appliance 6.0 by Using the GUI

  You can use the GUI installer to perform an interactive upgrade of a Platform Services Controller High Availability (HA) appliance 6.0 to version 6.7. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

- Upgrade a vCenter 6.5 HA Cluster 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 HA cluster 6.5 that uses an external vCenter Single Sign-On or Platform Services Controller instance to vCenter Server Appliance 6.7 with an external Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

Prerequisites for Upgrading vCenter Server High Availability Environments

To ensure a successful upgrade of vCenter Server or Platform Services Controller in a high availability (HA) environment, your environment must meet certain prerequisites before running the upgrade.

General Prerequisites

Ensure that your environment meets the prerequisites for upgrading vCenter Server Appliance and Platform Services Controller appliance. See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.

High Availability Prerequisites

In addition to the prerequisites for upgrading a standard vCenter Server Appliance, the vCenter High Availability (vCenter HA) upgrade has the following prerequisites.

- A vCenter HA cluster consists of three vCenter Server Appliances that act as Active, Passive, and Witness nodes. The Active node must be configured as the vCenter HA node.
- The Active node is part of the vCenter HA cluster.

- All nodes must be present in the cluster.
- The vCenter HA cluster must be in a healthy state.
- The vCenter HA cluster must be in enabled mode.
- The host that has the vCenter Server virtual machine (VM) must be managed by a container vCenter Server. It must not be standalone.
- The target vCenter Server must have the same placement as the source vCenter Server.
- vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

To learn more about vCenter HA configuration, see *vSphere Availability*.

Upgrade a vCenter Server Appliance 6.5 HA Cluster with an Embedded vCenter Platform Services Controller by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server Appliance 6.5 in a High Availability (HA) cluster that uses an embedded vCenter Single Sign-On or Platform Services Controller to vCenter Server Appliance 6.7 with an embedded Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

You can deploy version 6.7of the vCenter Server Appliance and Platform Services Controller appliance on hosts that are running ESXi 6.0 or later and on vCenter Server instances 6.0 or later.

A vCenter HA cluster consists of three vCenter Server Appliances that act as Active, Passive, and Witness nodes. The Active vCenter HA node is upgraded using a migration-based upgrade while preserving the existing configuration.

Prerequisites

- See Prerequisites for Upgrading vCenter Server High Availability Environments.
- See Required Information for Upgrading a vCenter Server Appliance 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.

Procedure

1. Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster

   In stage 1 of the upgrade process, you deploy the OVA file for the new vCenter Server Appliance and Platform Services Controller.

2. Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster

   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. When the deployment finishes, vCenter Server Appliance has high availability protection.

Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster

In stage 1 of the upgrade process, you deploy the OVA file for the new vCenter Server Appliance and Platform Services Controller.

Prerequisites

Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.

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 Connect to the source appliance that you want to upgrade. This appliance is the Active vCenter HA node.

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 Active vCenter HA node 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*.
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 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 Active node. The Active node must be configured as the vCenter HA node.
HTTPS port	If the 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.

5 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.

6 If vCenter HA is successfully detected, the target appliance is set to the manager of the source appliance. Click **OK**.

The appliance deployment target information is populated.

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 sign (@), or brackets (()).

Note The root password of the source is not transferred to the target appliance.

8 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

9 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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 GB of storage.

10 From the list of available datastores, select the location to store the virtual machine (VM) configuration files and virtual disks, and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

Note vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

11 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.
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.

12 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.

13 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.

The newly deployed vCenter Server Appliance 6.7 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 Data and Set-Up the Newly Deployed vCenter High Availability Cluster

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. When the deployment finishes, vCenter Server Appliance has high availability protection.

Prerequisites

Understand the data migration options available to you when upgrading or migrating to a vCenter Server Appliance with an embedded PostgreSQL database. You can select to migrate historical and other types of data in the background after deploying and starting vCenter Server Appliance. See Transferring Data from an Existing vCenter Server Appliance.

Procedure

1. Review the introduction to stage 2 of the deployment 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 migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server Appliance.
4. 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*.
5. On the Ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
6. Read the shutdown warning message and click **OK**.

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

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

After the Active node is upgraded, Auto Deployment automatically creates new Passive and Witness nodes using a clone operation. For Manual Deployment, nodes are not created automatically. You must clone the Passive and Witness virtual machines, and set the cluster mode to **Enabled**.

When the deployment finishes, vCenter Server Appliance has high availability protection. You can click **Edit** to enter Maintenance Mode, Disable, or Remove vCenter HA. You can also Initiate vCenter HA failover.

What to do next

For information about configuring and managing vCenter HA, see *vSphere Availability*.

Upgrade a Platform Services Controller High Availability Appliance 6.0 by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a Platform Services Controller High Availability (HA) appliance 6.0 to version 6.7. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

When upgrading multiple instances of Platform Services Controller configured in a HA environment, you upgrade the instances one by one in sequence. The following steps provide a high-level outline of the upgrade sequence.

1 From the load balancer, disable monitoring and node membership on the primary Platform Services Controller node, and redirect all connecting clients to the secondary Platform Services Controller node.

2 Upgrade the primary Platform Services Controller node.

3 After you finish the upgrade, re-enable traffic to the primary Platform Services Controller node.

4 Repeat this sequence to upgrade the secondary Platform Services Controller node, and any other HA nodes in your environment.

5 After you have finished upgrading all the Platform Services Controller nodes, start the services on all the nodes.

For more information on upgrading Platform Services Controller 6.0 or 6.5 to Platform Services Controller 6.7 in a High Availability (HA) environment, see Knowledge Base article KB 53661. For information on Platform Services Controller compatibility regarding the use of qualified load balancers that provide a high availability service, and their requirements between versions of vSphere, see Knowledge Base article KB 2112736.

Note vCenter Server deployments using an external Platform Services Controller will not be supported in a future vSphere release. Deploy or upgrade to a vCenter Server deployment using an embedded Platform Services Controller. For more information, see Knowledge Base article KB 60229.

Prerequisites

- See Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.

Procedure

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

   With stage 1 of the upgrade process, you deploy the OVA file of the new Platform Services Controller HA appliance 6.7.

2. Stage 2 - Transfer the Data and Set Up the Newly Deployed Platform Services Controller HA 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 6.7.

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

With stage 1 of the upgrade process, you deploy the OVA file of the new Platform Services Controller HA appliance 6.7.

Prerequisites

- Verify that a backup of the Platform Services Controller appliances exists for all Platform Services Controller instances you are upgrading.
- When upgrading an HA environment, you must first upgrade the Platform Services Controller instances configured for HA. From the load balancer, disable monitoring and node membership on the primary Platform Services Controller node, and redirect all connecting clients to the secondary Platform Services Controller node. For more information, see your load balancer vendor's documentation.

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	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with Platform Services Controller version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

   b. Enter the **Appliance (OS) Root password**.
   c. Enter the information about the 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 virtual machine** 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**. NFS datastores are thin provisioned by default.

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 begin 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 data from the old appliance, and set up the services of the new appliance.

Note If you exit the **Installer 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.

The newly deployed Platform Services Controller appliance 6.7 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.

What to do next

Transfer the data and set up the newly deployed Platform Services Controller HA Appliance.

Stage 2 - Transfer the Data and Set Up the Newly Deployed Platform Services Controller HA 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 6.7.

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.

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

Repeat this procedure to upgrade the secondary Platform Services Controller HA node, and any other HA nodes in your environment.

1 Re-enable traffic to the primary Platform Services Controller node.

2 From the load balancer, disable monitoring and node membership on the secondary Platform Services Controller node, and redirect all connecting clients to the primary Platform Services Controller node.

3 Upgrade the secondary Platform Services Controller node.

4 After you finish the upgrade, re-enable traffic to the secondary Platform Services Controller node, and re-enable health monitoring on the load balancer.

5 After you have upgraded all the Platform Services Controller HA nodes, start the services on all the nodes.

6 To configure the Platform Services Controller nodes for load balancing, run the `updateSSOConfig.py` and `updateLsEndpoint.py` scripts. See Knowledge Base article KB 2147384.

- 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 6.5 HA Cluster 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 HA cluster 6.5 that uses an external vCenter Single Sign-On or Platform Services Controller instance to vCenter Server Appliance 6.7 with an external Platform Services Controller. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

A vCenter HA cluster consists of three vCenter Server Appliances that act as Active, Passive, and Witness nodes. The Active vCenter HA node is upgraded using a migration-based upgrade while preserving the existing configuration.

Prerequisites

- Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.
- See Required Information for Upgrading a vCenter Server Appliance 6.0 or 6.5 or Platform Services Controller Appliance 6.0 or 6.5.
- Upgrade or migrate the external Platform Services Controller 6.0 instances in the domain to Platform Services Controller 6.7.

Procedure

1 Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster with an External Platform Services Controller

With stage 1 of the upgrade process, you deploy the OVA file of the new vCenter Server Appliance 6.7 with an external Platform Services Controller.

2 Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster 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. When the deployment finishes, vCenter Server Appliance has high availability protection.

Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster with an External Platform Services Controller

With stage 1 of the upgrade process, you deploy the OVA file of the new vCenter Server Appliance 6.7 with an external Platform Services Controller.

Prerequisites

Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.

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. This appliance is the Active vCenter HA node.

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 Active vCenter HA node 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*.
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 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 Active node. The Active node must be configured as the vCenter HA node.
HTTPS port	If the 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 vCenter Server HA is successfully detected, the target appliance is set to the manager of the source appliance. Click OK.

The appliance deployment target information is populated.

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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 GB of storage.

12 From the list of available datastores, select the location to store the virtual machine (VM) configuration files and virtual disks, and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

Note vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

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.

The newly deployed target vCenter Server Appliance 6.7 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.

What to do next

Transfer the data from the old appliance and start the services of the newly deployed vCenter Server Appliance 6.7 with an external Platform Services Controller See Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster with an External Platform Services Controller.

Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster 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. When the deployment finishes, vCenter Server Appliance has high availability protection.

Prerequisites

Understand the data migration options available to you when upgrading or migrating to a vCenter Server Appliance with an embedded PostgreSQL database. You can select to migrate historical and other types of data in the background after deploying and starting vCenter Server Appliance. See Transferring Data from an Existing vCenter Server Appliance.

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 migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server Appliance.
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.

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

After the Active node is upgraded, a new Passive and Witness node is created using a clone operation. These nodes are created automatically for Auto Deployment. For Manual Deployment, nodes are not created automatically. You must clone the Passive and Witness VMs and set the cluster mode to **enabled**.

When the deployment finishes, vCenter Server Appliance has high availability protection. You can click **Edit** to enter Maintenance Mode, Disable, or Remove vCenter HA. You can also Initiate vCenter HA failover.

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-6.7.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-6.7.0.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 4-9. Upgrade JSON Templates Included in the vCenter Server Appliance Installer

Location	Template	Description
`vcsa-cli-installer\templates\upgrade\vcsa\6.0`	`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 6.7 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 6.7 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 6.7 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 6.7 on a vCenter Server instance.

Table 4-9. Upgrade JSON Templates Included in the vCenter Server Appliance Installer (Continued)

Location	Template	Description
	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 6.7 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 6.7 with an external Platform Services Controller on a vCenter Server instance.
vcsa-cli-installer\templates\upgrade\vcsa\6.5	embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.5 with an embedded Platform Services Controller to vCenter Server Appliance 6.7 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 6.5 with an embedded Platform Services Controller to vCenter Server Appliance 6.7 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 6.5 to Platform Services Controller appliance 6.7 on an ESXi host.
	PSC_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a Platform Services Controller appliance 6.5 to Platform Services Controller appliance 6.7 on a vCenter Server instance.

Table 4-9. Upgrade JSON Templates Included in the vCenter Server Appliance Installer (Continued)

Location	Template	Description
	vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server Appliance 6.5 with an external Platform Services Controller to vCenter Server Appliance 6.7 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 6.5 with an external Platform Services Controller to vCenter Server Appliance 6.7 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 4-10. 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 4-11. **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 4-12. **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 4-13
	os	Contains only the ssh_enable configuration parameter to set the SSH administrator login to the new appliance.

Table 4-10. Sections and Subsections of Configuration Parameters in the JSON Upgrade Files (Continued)

Section	Subsection	Description
	`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.
	`temporary_network`	Contains the configuration parameters that describe the temporary network settings for the new appliance. See Table 4-14
	`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 4-15
`source_vc` - describes the existing appliance that you want to upgrade	`managing_esxi_or_vc`	Contains the configuration parameters that describe the source ESXi host or vCenter Server Appliance instance on which resides the appliance that you want to upgrade. See Table 4-16.
	`vc_vcsa`	Contains the configuration parameters that describe the source appliance that you want to upgrade. See Table 4-17.
`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 4-18. **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 4-19. Required only if you are upgrading a vCenter Server Appliance with an embedded Platform Services Controller 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-6.7.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-6.7.0.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 4-11. 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 be part of the target ESXi host or vCenter Server Appliance instance (as identified by the `managing_esxi_or_vc` configuration parameter) network configuration. **Note** The network must be accessible from the source ESXi host or vCenter Server Appliance instance (as identified by the `managing_esxi_or_vc` configuration parameter) 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.

Table 4-11. Configuration Parameters in the `new_vcsa` Section, `esxi` Subsection (Continued)

Name	Type	Description
`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.

`ssl_certificate_verification`	string	The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI will stop the upgrade unless you specify one of the following SSL certificate configuration options:
		Specify the Secure Hash Algorithm 1 (SHA-1) certificate thumbprint. A certificate thumbprint is a hexadecimal string that uniquely identifies a certificate. The thumbprint is calculated from the content of the certificate using a thumbprint algorithm.
		`"thumbprint": "certificate SHA-1 thumbprint"`
		Set `verification_mode` to `NONE`.
		`"verification_mode": "NONE"`
		If you are connecting to a server with a self-signed certificate, and fail to either specify the SHA-1 certificate thumbprint or set the verification mode to `NONE`, the CLI will display the server's self-signed cert's thumbprint, and prompt you to accept or reject the certificate thumbprint.
		You may also specify that the CLI ignore the self-signed using the `vcsa-deploy upgrade` command parameter `--no-ssl-certificate-validation`. See Syntax of the CLI Upgrade Command .

Table 4-12. 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.
`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.

Table 4-12. Configuration Parameters in the `new_vcsa` Section, `vc` Subsection (Continued)

Name	Type	Description

`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"`
		If there is no folder path on the datacenter, then use only the datacenter name. For example,
		`["datacenter_name"]`
		or
		`"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 4-12. Configuration Parameters in the `new_vcsa` Section, `vc` Subsection (Continued)

Name	Type	Description

`target`	string or array	The target cluster, ESXi host, or resource pool on which you want to deploy the new appliance. This is the target you specified with the `datacenter` parameter. This path must end with a cluster name, ESXi hostname, or resource pool name.
		
		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.
		
		Note All values are case-sensitive.
		
		If you want the deployed appliance to be listed in a different location within the data center's hierarchy, use the `vm_folder` parameter described below.
		If the target cluster, ESXi host, or resource pool 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"`
		If you are deploying to a resource pool, include the label `Resources` before the resource pool name. For example:
		`["cluster_name", "Resources", "resource_pool_name"]`
		
		Note Pre-checks verify only the memory of the resource pool.

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

Table 4-13. 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 300 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 825 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 1700 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 340 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 870 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 1750 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 525 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 1025 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 1905 GB of storage.

Table 4-13. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (Continued)

Name	Type	Description
		■ 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 740 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 1090 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 1970 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 1180 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 1230 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 2110 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 300 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, 10 GB of memory, and 825 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 1700 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 340 GB of storage.

Table 4-13. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (Continued)

Name	Type	Description
		■ 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 870 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 1750 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 525 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 1025 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 1905 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 740 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 1090 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 1970 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 1180 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 1230 GB of storage.

Table 4-13. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (Continued)

Name	Type	Description
		■ 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 2110 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 4-14. 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.

Table 4-14. Configuration Parameters in the `new_vcsa` Section, `temporary_network` Subsection (Continued)

Name	Type	Description

`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`.
`gateway`	string	IP address of the default gateway for the temporary network of the new appliance. For IPv6 version, the value can be `default`.

Table 4-15. Configuration Parameters in the `new_vcsa` Section, `user_options` Subsection

Name	Type	Description
`vcdb_migrateSet`	string	Select the types of data to migrate from the old appliance to the new appliance. Data will be copied from the source vCenter Server to the target server. The original source of the data will remain unchanged. ■ Set to `core` if you want to transfer only the configuration data. This option provides the fastest data migration, keeping system downtime to a minimum. ■ Set to `core_events_tasks` if you want to transfer the configuration and historical data (events and tasks) immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Appliance. ■ Set to `all` if you want to transfer the configuration, historical, and performance metrics data immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. This option transfers the largest amount of data, and requires more downtime than other data migration options. ■ Set to `transfer_events_tasks_after_upgrade` if you want to transfer the historical data (events and tasks) in the background after the upgrade completes. During this time, vCenter Server performance may not be optimal. ■ Set to `transfer_stats_events_tasks_after_upgrade` if you want to transfer historical data and performance metrics data in the background after the upgrade completes. During this time, vCenter Server performance may not be optimal. **Note** To minimize upgrade time and the amount of storage required for the new vCenter Server appliance, use the `core` value. For more information on the types of data you can transfer from your existing vCenter Server to the new, upgraded vCenter Server, see Transferring Data from an Existing vCenter Server Appliance.

Configuration Parameters in the `source_vc` Section

Table 4-16. Configuration Parameters in the `source_vc` Section, `managing_esxi_or_vc` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the source ESXi or vCenter Server 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 4-17. 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*.
`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 4-18. 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 4-19. 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 Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are running the upgrade on 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 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. This example also confirms participation in the VMware Customer Experience Improvement Program (CEIP). If the `ceip_enabled` parameter is set to true in the JSON deployment template, you must include the argument `--acknowledge-ceip`.

```
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*	Specifies the location of the log and other output files that the installer generates.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters and deploys the vCenter Server appliance, but does not validate the OVF Tool parameters in the `ovftool_arguments` subsection of the JSON template. If you set arguments that the OVF Tool does not recognize, the deployment might fail.

Argument	Description
`--no-ssl-certificate-verification`	Prohibits SSL verification of for all server connections. The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI stops the upgrade unless you specify that the CLI ignore the self-signed certificate using the `--no-ssl-certificate-validation` command parameter. If you are connecting to a server with a self-signed certificate, and fail to specify that the CLI accept it, the CLI displays the server's self-signed certificate thumbprint, and prompts you to accept or reject the it. You can also specify that the CLI ignore self-signed certificates using the `ssl_certificate_verification` configuration parameter in the JSON template. See Upgrade Configuration Parameters. **Important** Avoid using this option as it may cause problems during or after upgrade due to an un-validated identity of the target host.
`--operation-id`	Lets you provide an identifier to track the concurrent installation, migration, or upgrade of multiple vCenter Server instances. If do not provide an operation ID, the CLI generates a universally unique identifier (UUID) which you can use to identify the different instances of vCenter Server and their installation or upgrade status.
`--pause-on-warnings`	Pauses and waits for acknowledgment of warnings.
`--verify-template-only`	Performs basic template verification without installing Upgrade Runner, running prechecks, and upgrading or migrating the vCenter Server 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

Migrating vCenter Server for Windows to vCenter Server Appliance

5

You can migrate a vCenter Server installation on Windows to a vCenter Server Appliance installation while upgrading to version 6.7.

This chapter includes the following topics:

Overview of Migration from vCenter Server on Windows to an Appliance

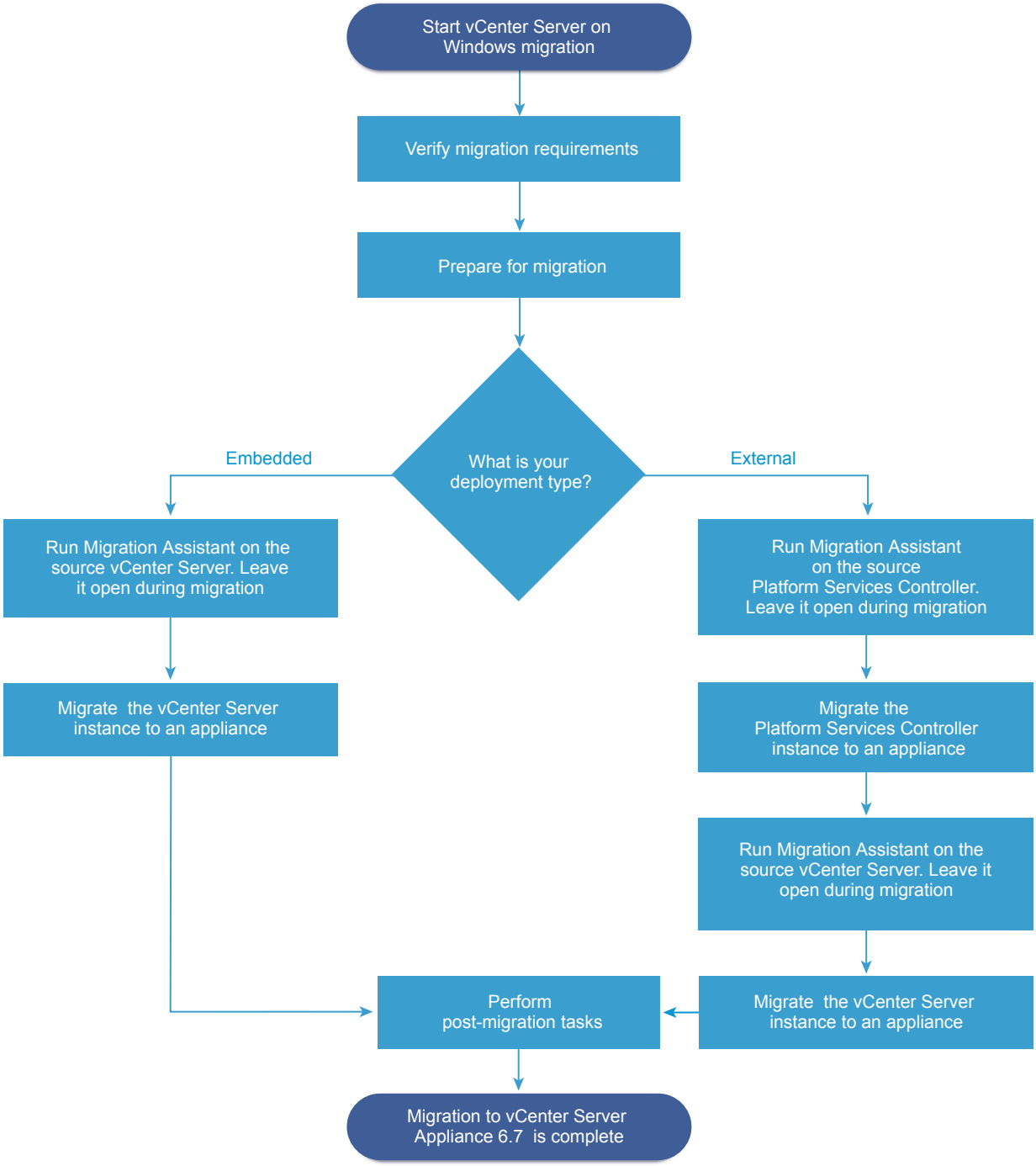
VMware provides supported paths for migrating from vCenter Server version 6.0 and version 6.5 installations on Windows to vCenter Server Appliance 6.7 installations.

You can migrate the following deployments:

Table 5-1. Supported vSphere Migration Paths

Source Configuration	Target Configuration
vCenter Server 6.0 with an Platform Services Controller embedded instance on Windows	vCenter Server Appliance 6.7 with an embedded Platform Services Controller appliance
vCenter Server 6.5 with an embedded Platform Services Controller instance on Windows	
Platform Services Controller 6.0 instance on Windows	External Platform Services Controller 6.7 appliance
Platform Services Controller 6.5 instance on Windows	
vCenter Server 6.0 instance on Windows	vCenter Server Appliance 6.7 with an external Platform Services Controller appliance
vCenter Server 6.5 instance on Windows	

Figure 5-1. High-level Tasks for vCenter Server on Windows Migration to vCenter Server Appliance 6.7



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 6.7

For vSphere 6.5 and later releases, Update Manager is delivered as a 64-bit application and can be installed only on a 64-bit Windows operating system. In vSphere 6.5 and 6.7, Update Manager is provided as an optional service in the vCenter Server Appliance 6.7. VMware provides supported paths for migrating Update Manager from a Windows operating system to a vCenter Server Appliance 6.7.

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

Table 5-2. 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 6.7 with embedded Update Manager
vCenter Server and Update Manager run on different Windows machines	vCenter Server Appliance 6.7 with embedded Update Manager
Update Manager run on a Windows machine and is connected to a vCenter Server Appliance	vCenter Server Appliance 6.7 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, Oracle, or embedded database solutions. After the migration to the vCenter Server Appliance, Update Manager uses 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 or Platform Services Controller on Windows to an appliance, the installer performs a pre-check of the environment to ensure it meets requirements. For example, the pre-check verifies that enough space is available on the virtual machine or physical server where you are migrating, and that the external database, if any, can be successfully accessed.

Source Environment Checks

When you migrate Platform Services Controller (version 6.0 or 6.5), 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 or Platform Services Controller 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 6.7. 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 6.7 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, Update Manager, vSphere ESXi Dump Collector, and HTTP reverse proxy (RHTTP) 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.

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 physical machines in your vSphere network are not synchronized, SSL certificates and SAML Tokens, 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 `vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause firstboot to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server Appliance is not synchronized with NTP. Similarly, issues can arise if the destination vCenter Server Appliance migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server Appliance.

- The target ESXi host where the destination vCenter Server Appliance is to be deployed is synchronized to NTP.
- The ESXi host running the source vCenter Server Appliance is synchronized to NTP.
- When upgrading or migrating, if the vCenter Server Appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP.
- If you are upgrading or migrating, verify that the source vCenter Server or vCenter Server Appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See Knowledge Base article 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*.

To learn how to change time synchronization settings for vCenter Server Appliance, see "Configuring Time Synchronization Settings in the vCenter Server Appliance" in *vCenter Server Appliance Configuration*.

To learn how to edit time configuration for a host, see "Edit Time Configuration for a Host" in *vCenter Server and 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.
- 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 Make a full backup of the vCenter Server database.

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 Make a full backup of the vCenter Server database.

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.

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 6.7.
- 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 6.0 or greater. If your ESXi hosts are version 5.5 or earlier, upgrade them to 6.0 or 6.5. Read and follow all best practices when upgrading your ESXi hosts.
- 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 6.7.

   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**.

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 5-3. 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.

Note Visual C++ redistributable libraries need to be installed to run the CLI installer on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa-cli-installer/win32/vcredist` directory.

Note Deploying the vCenter Server Appliance with the GUI requires a minimum resolution of 1024x768 to properly display. Lower resolutions can truncate the UI elements.

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.

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 perform a set of required tasks and pre-checks prior to 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.
- 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.
- Back up the source machine that you want to migrate as a precaution in case of failure during the migration process.
- 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 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 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*.

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 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 a 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 5-4. 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`	

Table 5-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
	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	
	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		

Table 5-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
	vCenter Server Appliance size. The options vary depending on the size of your vSphere environment. ■ Tiny (up to 10 hosts, 100 virtual machines) ■ Small (up to 100 hosts, 1,000 virtual machines) ■ Medium (up to 400 hosts, 4,000 virtual machines) ■ Large (up to 1,000 hosts, 10,000 virtual machines) ■ X-Large (up to 2,000 hosts, 35,000 virtual machines)	Tiny (up to 10 hosts, 100 virtual machines)	

Table 5-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
	Storage size of the vCenter Server Appliance for your vSphere environment. Increase the default storage size if you want larger volume for SEAT data (stats, events, alarms, and tasks). ■ 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.	Default	

Table 5-4. Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance (Continued)

Required Information		Default Value	Your Entry
	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.		
	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 Platform Services Controller to a vCenter Server Appliance with an embedded Platform Services Controller appliance.

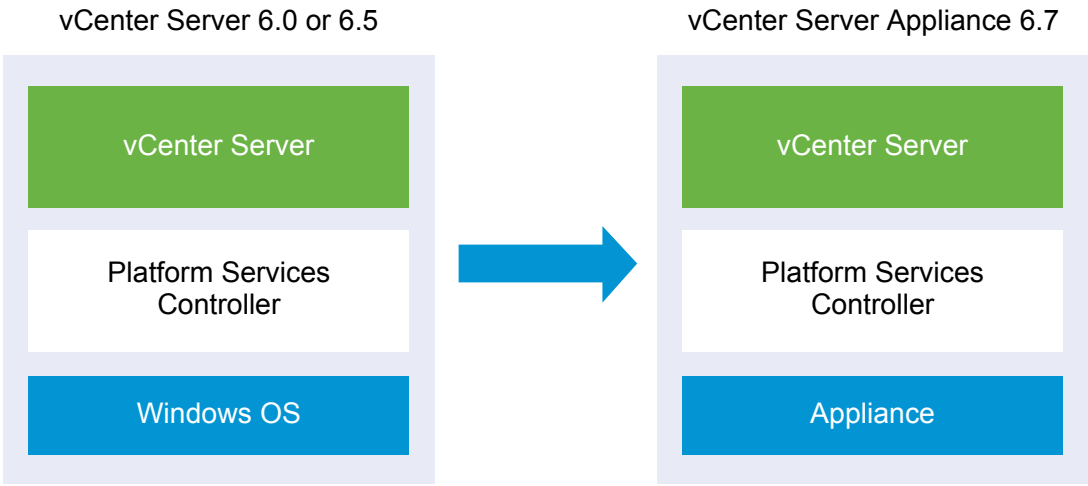
When you migrate from vCenter Server with an embedded Platform Services Controller (version 6.0 or 6.5) on Windows to vCenter Server Appliance with an embedded Platform Services Controller appliance, the entire deployment is migrated in only one step.

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 Platform Services Controller from Windows to an appliance.

Figure 5-2. vCenter Server 6.0 or 6.5 with Embedded Platform Services Controller Deployment Before and After Migration



GUI tasks for migrating vCenter Server with an embedded 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.

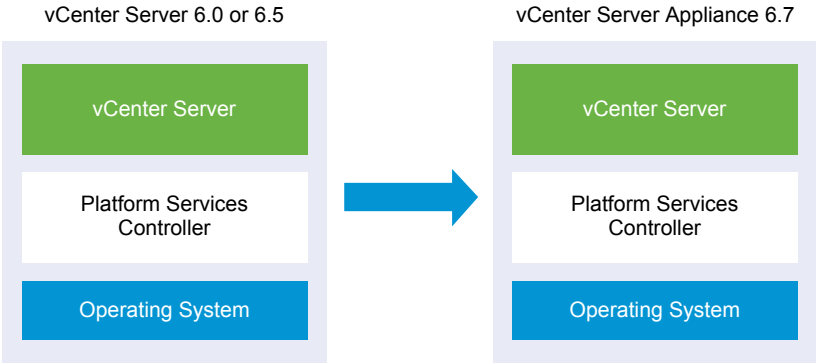
The installer:

- 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 5-3. vCenter Server 6.0 or 6.5 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 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.

6 (Optional) Review the warning message and try to resolve the warnings, if any, and click **Yes**.

7 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**.

8 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.

9 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.

10 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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 GB of storage.

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**. NFS datastores are thin provisioned by default.

12 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.

13 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.

14 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.

The newly deployed target vCenter Server Appliance 6.7 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 6.7 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.

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 6 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 Platform Services Controller (version 6.0 or 6.5) on Windows to vCenter Server Appliance with an external Platform Services Controller appliance, you migrate in two steps.

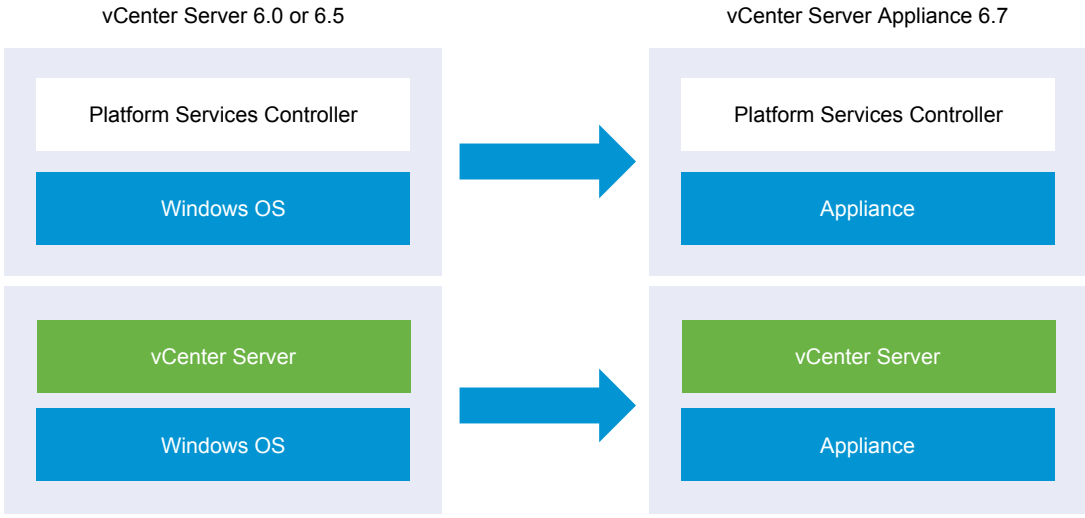
If you use Update Manager in the vCenter Server deployment on Windows that you migrate, and Update Manager runs on a separate machine from any other of the vCenter Server components, take an extra step to migrate Update Manager to an appliance.

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 5-4. vCenter Server 6.0 or 6.5 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 or 6.5 appliance, you upgrade the Platform Services Controller appliance to the version 6.7 appliance 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 6.7.

Important Concurrent migrations of 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 you use to log in to the physical machine from which you want to run the GUI installer, the path to the vCenter Server Appliance installer, and values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

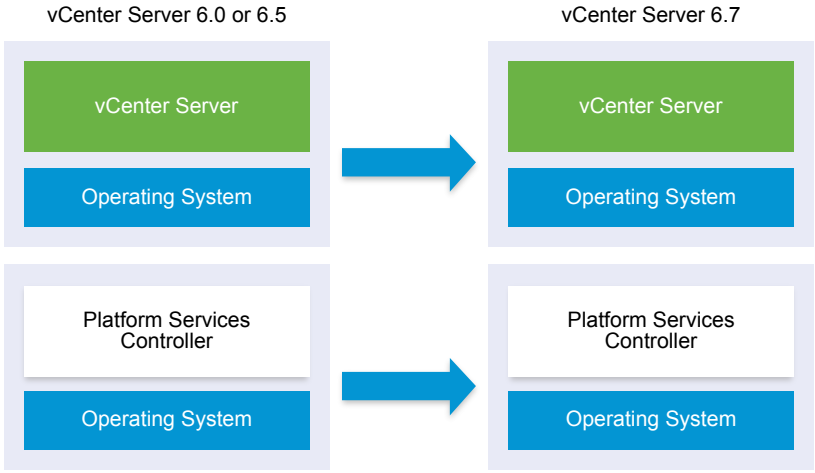
For each node to be migrated, the installer:

- Deploys a new target appliance.
- Exports the required files from the source 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 indicated in the Summary.
- Imports and updates the files and settings of the source 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 5-5. vCenter Server 6.0 or 6.5 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 thePlatform 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**. NFS datastores are thin provisioned by default.

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 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.

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 Platform Services Controller instance and set up the services.

The newly deployed Platform Services Controller appliance 6.7 is running on the target server but is not configured.

Important The data from the source 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.

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.

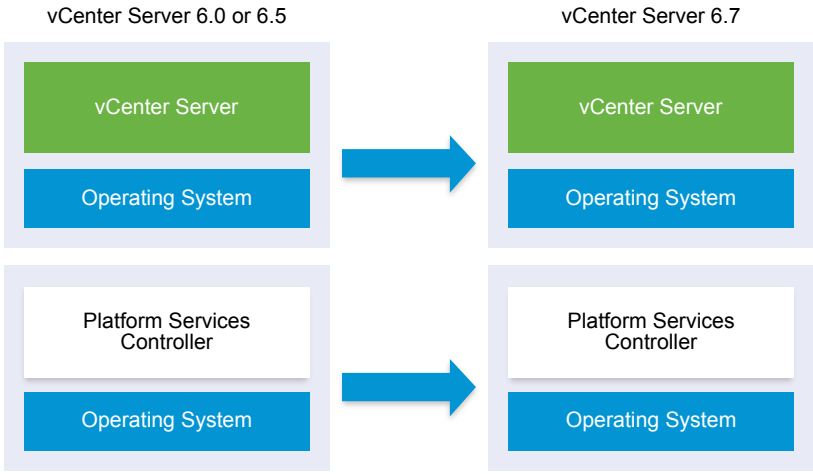
For the new Platform Services Controller appliance to replicate infrastructure data with other Platform Services Controller instances, you must migrate or upgrade all joined Platform Services Controller instances within the vCenter Single Sign-On domain to the same version. For information on upgrading Platform Services Controller instances on Windows, see Upgrade vCenter Platform Services Controller 6.0 or 6.5 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 6.0 or 6.5 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 5-6. vCenter Server 6.0 or 6.5 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 300 GB of storage.	Deploys an appliance with 340 GB of storage.	Deploys an appliance with 525 GB of storage.	Deploys an appliance with 740 GB of storage.	Deploys an appliance with 1180 GB of storage.
Large	Deploys an appliance with 825 GB of storage.	Deploys an appliance with 870 GB of storage.	Deploys an appliance with 1025 GB of storage.	Deploys an appliance with 1090 GB of storage.	Deploys an appliance with 1230 GB of storage.
X-Large	Deploys an appliance with 1700 GB of storage.	Deploys an appliance with 1750 GB of storage.	Deploys an appliance with 1905 GB of storage.	Deploys an appliance with 1970 GB of storage.	Deploys an appliance with 2110 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**. NFS datastores are thin provisioned by default.

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.

The newly deployed target vCenter Server Appliance 6.7 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.

Prerequisites

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.

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 6.0 or 6.5 on Windows.

For post-migration steps, see Chapter 6 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, or you can run the CLI migrations concurrently in a batch mode.

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 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 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 6.0 and vCenter Server 6.5 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.

To perform the batch migration, place the JSON templates defining your deployment in a single directory. When invoked, the CLI installer migrates your existing deployment to the new vCenter Server version using the topology defined in the JSON templates.

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 6.0, use the `migrate/winvc6.0/` folder.
   - For vCenter Server 6.5, use the `migrate/winvc6.5/` 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.

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 5-5. 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.

Table 5-5. Sections and Subsections of Configuration Parameters in the JSON Migration Templates (Continued)

Section	Subsection	Description
	`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 or Platform Services Controller
	`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 Platform Services Controller 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 5-6. 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.

Table 5-6. Configuration Parameters in the new_vcsa Section, esxi Subsection (Continued)

Name	Type	Description
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.

ssl_certificate_verification	string	The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI will stop the upgrade unless you specify one of the following SSL certificate configuration options.
		Specify the Secure Hash Algorithm 1 (SHA-1) certificate thumbprint. A certificate thumbprint is a hexadecimal string that uniquely identifies a certificate. The thumbprint is calculated from the content of the certificate using a thumbprint algorithm.
		`"thumbprint": "certificate SHA-1 thumbprint"`
		Set verification_mode to NONE.
		`"verification_mode": "NONE"`
		If you are connecting to a server with a self-signed certificate, and fail to either specify the SHA-1 certificate thumbprint or set the verification mode to NONE, the CLI will display the server's self-signed cert's thumbprint, and prompt you to accept or reject the certificate thumbprint.
		You may also specify that the CLI ignore the self-signed using the vcsa-deploy upgrade command parameter --no-ssl-certificate-validation. See Syntax of the CLI Migrate Command .

Table 5-7. 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.

Table 5-7. Configuration Parameters in the `new_vcsa` Section, `vc` Subsection (Continued)

Name	Type	Description

`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"`
		If there is no folder path on the datacenter, then use only the datacenter name. For example,
		`["datacenter_name"]`
		or
		`"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 25 GB of free space.
`port`	integer	The port number of the vCenter Server. The default port is 443.

Table 5-7. Configuration Parameters in the `new_vcsa` Section, `vc` Subsection (Continued)

Name	Type	Description

`target`	string or array	The target cluster, ESXi host, or resource pool on which you want to deploy the new appliance. This is the target you specified with the `datacenter` parameter. This path must end with a cluster name, ESXi hostname, or resource pool name.
		
		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.
		
		Note All values are case-sensitive.
		
		If you want the deployed appliance to be listed in a different location within the data center's hierarchy, use the `vm_folder` parameter described below.
		If the target cluster, ESXi host, or resource pool 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"`
		If you are deploying to a resource pool, include the label `Resources` before the resource pool name. For example:
		`["cluster_name", "Resources", "resource_pool_name"]`
		
		Note Pre-checks verify only the memory of the resource pool.

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

Table 5-8. 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, 10 GB of memory, and 300 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 825 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 1700 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 340 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 870 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 1750 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 525 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 1025 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 1905 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 740 GB of storage.

Table 5-8. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (Continued)

Name	Type	Description
		■ 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 1090 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 1970 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 1180 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 1230 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 2110 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 300 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, 10 GB of memory, and 825 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 1700 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 340 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 870 GB of storage.

Table 5-8. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (Continued)

Name	Type	Description
		■ 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 1750 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 525 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 1025 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 1905 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 740 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 1090 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 1970 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 1180 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 1230 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 2110 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.

Table 5-8. Configuration Parameters in the new_vcsa Section, appliance Subsection (Continued)

Name	Type	Description
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 5-9. 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 5-10. 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.

Table 5-10. Configuration Parameters in the `new_vcsa` Section, `temporary_network` Subsection (Continued)

Name	Type	Description

`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`.

Table 5-11. Configuration Parameters in the `new_vcsa` Section, `user_options` Subsection

Name	Type	Description
`vcdb_migrateSet`	string	Select the types of data to migrate from the old appliance to the new appliance. Data will be copied from the source vCenter Server to the target server. The original source of the data will remain unchanged. ■ Set to `core` if you want to transfer only the configuration data. This option provides the fastest data migration, keeping system downtime to a minimum. ■ Set to `core_events_tasks` if you want to transfer the configuration and historical data (events and tasks) immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. ■ Set to `all` if you want to transfer the configuration, historical, and performance metrics data immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. This option transfers the largest amount of data, and requires more downtime than other data migration options. ■ Set to `transfer_events_tasks_after_upgrade` if you want to transfer the historical data (events and tasks) in the background after the upgrade completes. During this time, vCenter Server performance may not be optimal. ■ Set to `transfer_stats_events_tasks_after_upgrade` if you want to transfer historical data and performance metrics data in the background after the upgrade completes. During this time, vCenter Server performance may not be optimal. **Note** To minimize migration time and the amount of storage required for the new vCenter Server appliance, use the `core` value. For more information on the types of data you can transfer from your existing vCenter Server to the new, upgraded vCenter Server, see Transferring Data from an Existing vCenter Server Appliance.

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 needs 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* or *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 5-12. 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 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 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.
`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 5-13. 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.

Table 5-13. Configuration Parameters in the source_vc Section, run_migration_assistant Subsection (Continued)

Name	Type	Description
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 5-14. 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.
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 5-15. 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. Verify your template without deploying the appliance by entering the command: `vcsa-deploy migrate --verify-template-only` *`path_to_json_file`*.
2. Run `CLI Migrate` using the `--precheck-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.
3. After resolving any errors, run the `CLI Migrate` command using the `--verify-template-only` option again until all errors are resolved.

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-6.7.0-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
   ```

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. You can place multiple JASON files in a directory, and the CLI will migrate all of the deployments in batch mode. For more information on performing concurrent migrations, see Prepare JSON Configuration Files for CLI Migration.

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.
`-t`, `--terse`	Hides the console output. Displays only warning and error messages.
`--log-dir`, `LOG_DIR`	Specifies the location of the log and other output files that the installer generates.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters and deploys the vCenter Server appliance, but does not validate the OVF Tool parameters in the `ovftool_arguments` subsection of the JSON template. If you set arguments that the OVF Tool does not recognize, the deployment might fail.

Optional Argument	Description
`--no-ssl-certificate-verification`	Prohibits SSL verification of ESXi connections. The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI will stop the upgrade unless you specify that the CLI ignore the self-signed certificate using the `--no-ssl-certificate-validation` command parameter. If you are connecting to a server with a self-signed certificate, and fail to specify that the CLI accept it, the CLI displays the server's self-signed certificate thumbprint, and prompts you to accept or reject the it. You can also specify that the CLI ignore self-signed certificates using the `ssl_certificate_verification` configuration parameter in the JSON template. See Upgrade Configuration Parameters. **Important** Avoid using this option as it may cause problems during or after upgrade due to an un-validated identity of the target host.
`--operation-id`	Lets you provide an identifier to track the concurrent installation, migration, or upgrade of multiple vCenter Server instances. If do not provide an operation ID, the CLI generates a universally unique identifier (UUID) which you can use to identify the different instances of vCenter Server and their installation or upgrade status.
`--verify-template-only`	Performs basic template verification without installing Upgrade Runner, running prechecks, and upgrading or migrating the vCenter Server Appliance.
`--precheck-only`	Installs Migration Assistant on the source vCenter Server virtual machine, 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

6

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

- You can review the database upgrade logs. See Collect Database Upgrade Logs.
- Complete any component reconfigurations that might be required for changes during upgrade.
- Verify that you understand the authentication process and identify your identity sources.
- 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
- Monitor and Manage Historical Data 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.

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 Client

Log in to vCenter Server by using the vSphere Client to manage your vSphere inventory.

In vSphere 6.5 and later, the vSphere Client is installed as part of the vCenter Server on Windows or the vCenter Server Appliance deployment. This way, the vSphere Client always points to the same vCenter Single Sign-On instance.

Procedure

1. Open a Web browser and enter the URL for your vCenter Server instance:
   `https://`*`vcenter_server_ip_address_or_fqdn`*

2 Select **Launch vSphere Client (HTML5)**. To use the vSphere Web Client, select **Launch vSphere Web Client (Flex)**.

   You can instead open a Web browser and enter the URL for the vSphere Client: **`https://vcenter_server_ip_address_or_fqdn/ui`**. To use the vSphere Web Client, enter the URL: **`https://vcenter_server_ip_address_or_fqdn/vsphere-client`**.

3 Enter the credentials of a user who has permissions on vCenter Server, and click **Login**.

4 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.

5 To log out, click the user name at the top of the vSphere Client window and select **Logout**.

The vSphere 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 the vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaced 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 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_web_client_after_cip_removal)

Install the plug-in only once to enable all the functionality the plug-in delivers.

If you install the plug-in from an Internet Explorer browser, you must first disable Protected Mode and enable pop-up windows on your Web browser. Internet Explorer identifies the plug-in as being on the Internet instead of on the local intranet. In such cases, the plug-in is not installed correctly because Protected Mode is enabled for the Internet.

For information about supported browsers and operating systems, see the *vCenter Server Installation and Setup* documentation.

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

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.

Uninstall the TLS Configuration Utility on Windows

You can remove the previous verison of the TLS Configuration utility.

vCenter Server 6.7 for Windows has its own version of the TLS Configuration utility that is installed when you perform an upgrade. However, the previous version of the TLS Configuration utility remains installed. You can manually remove this utility from your deployment.

Prerequisites

You have successfully upgraded your Windows-based vCenter Server to version 6.7.

Procedure

1. Locate the folder `C:\Program Files\VMware\CIS\TlsReconfigurator\VcTlsReconfigurator`.
2. Right-click the folder name or icon, and select **Delete** from the pop-up menu.
3. Verify that the TLS Configuration utility was removed.

What to do next

To learn more about the TLS Configuration utility, see the *vSphere Security* documentation.

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

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 administrator can add identity sources, set the default identity source, and create users and groups in the vsphere.local identity source.

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.

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 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 Client.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources. Shown as **OpenLDAP** in the vSphere 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 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.

For more information about vCenter Single Sign-On, see *Platform Services Controller Administration*.

Reregister Plug-In Solution in vCenter Server After Upgrade or Migration

You reregister a previously registered plug-in solution and any third-party client plug-in packages with vCenter Server after the SSL certificate has been refreshed following an upgrade or migration.

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.

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 Client extension.
5. To unregister the extension click **Invoke Method**.

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.

- In the vSphere 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 Client. The vSphere 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.

Monitor and Manage Historical Data Migration

You can monitor and mange the background migration of historical data using the vCenter Server Appliance Management Interface.

Using the vCenter Server Appliance Management Interface, you can perform the following data management tasks:

- Monitor the progress of the data migration.
- Pause the data migration.
- Cancel the data migration.

Prerequisites

- Verify that the vCenter Server Appliance is successfully deployed and running.
- You must have chosen to import historical data from the external database in use by the previous version of vCenter Server to the embedded PostgreSQL database in use by version 6.7 of the vCenter Server Appliance. See Transferring Data from an Existing vCenter Server Appliance.

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.
3. A status bar at the top of the vCenter Server Appliance Management Interface displays the percentage of data that has been copied from the source vCenter Server to the embedded PostgreSQL database in use by the target vCenter Server Appliance.
4. Click **Manage** to pause or cancel the data migration.

Option	Description
Pause	During the data migration, vCenter Server performance may not be optimal. Pausing the migration allows vCenter Server to run with better performance until such time that you can resume the process when it doesn't interfere with the needs of your business.
Resume	You can resume the data migration at a time that does not interfere with the business needs of your vCenter Server deployment.
Cancel	If you cancel the data import, the historical data will not be imported to the embedded PostgreSQL database. You cannot recover the data once you cancel the operation. If you cancel the import process, and wish to import the historical data at a later time, you must restart the upgrade or migration process from Stage 1 of the GUI installer.

When the data has been completely migrated, a success message displays in the vCenter Server Appliance Management Interface status bar.

Changing the vCenter Server Deployment Topology

7

After you upgrade vCenter Server, you can change the topology by either repointing the Platform Services Controller, or converting a vCenter Server instance with an external Platform Services Controller to a instance with an embedded Platform Services Controller.

This chapter includes the following topics:

Changing a vCenter Server Deployment Type After Upgrade or Migration

You can change your vCenter Server deployment type after upgrade or migration to version 6.7.

Repoint vCenter Server to Another External Platform Services Controller in the Same Domain

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.

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*.

Converging vCenter Server with an External Platform Services Controller to a vCenter Server with an Embedded Platform Services Controller

Convergence is the process of reconfiguring or converting a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with an embedded Platform Services Controller.

If you have deployed or upgraded a vCenter Server instance with an external Platform Services Controller, you can convert it to a vCenter Server instance with an embedded Platform Services Controller using either the vSphere Client, or the `vcsa-util` command line converge utility.

To learn more about converting a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with an embedded Platform Services Controller, see *vCenter Server Installation and Setup*.

Patching and Updating vCenter Server 6.7 Deployments

8

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

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.

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.
- If you are using Internet Explorer, verify that TLS 1.0, TLS 1.1, and TLS 1.2 are enabled in the security settings.

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 that you set while deploying the vCenter Server Appliance.

Check for and Stage Patches to the vCenter Server Appliance

Before you install available patches, you can stage the patches to the appliance. You can use the Appliance Management Interface 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 Log into the vCenter Server Appliance Management Interface as root.

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

2 Click **Update**.

3 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.

4 You can run a pre-check of an update to verify that it is compatible with your current deployment.

5 Click the staging option you would like to use.

Option	Description
Stage Only	Stages the selected patches to the appliance for installation at a later time.
Stage and Install	Stages and installs the selected patches to the appliance. For more information on installing patches, see Install vCenter Server Appliance Patches.

In the process of staging, the Appliance Management Interface 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.

What to do next

If you chose to stage the available patches for installation at a later time, you can now install. See Install vCenter Server Appliance Patches.

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

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

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

   c Extract the ZIP file into the repository directory.

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

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

3 Click **Settings**.

4 Select the Repository settings.

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

5 Click **OK**.

What to do next

Install vCenter Server Appliance Patches

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 *vCenter Server Installation and Setup*.

Prerequisites

- Log in to the vCenter Server Appliance Management Interface as root.
- Before you can install available patches, you check for new patches and stage the patches to the appliance. See Check for and Stage Patches to the vCenter Server Appliance.
- 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.

2 Select the range of stages patches to apply, and click **Install Updates**.

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

3 Read and accept the End User License Agreement.

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

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

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**.

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. Download the vCenter Server Appliance patch ZIP file from the VMware website at https://my.vmware.com/web/vmware/downloads.
   b. On your Web server, create a repository directory under the root.

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

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

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

   You can see information about the current repository URL, the default repository URL, the time at which the appliance last checked for patches, the time at which the appliance last installed patches, and the current configuration of automatic checks for patches.

4 Configure the current repository for URL-based patching.

- To configure the appliance to use the default VMware repository URL, run the following command:

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

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

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

where the square brackets [] enclose the command options.

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

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

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

where the square brackets [] enclose the command options.

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

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

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

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

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

What to do next

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

Stage Patches to the vCenter Server Appliance

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

Prerequisites

- If you are staging patches from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server Appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Web Client. See *vSphere Virtual Machine Administration*.
- If you are staging patches from a remote repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.

Procedure

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

The default user with a super administrator role is root.

2 Stage the patches.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
software-packages    unstage
```

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

What to do next

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

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

Install vCenter Server Appliance Patches

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

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

   - 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 directly accept the End User License Agreement, use the `--acceptEulas` option.

   For example, to install 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 --acceptEulas
   ```

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

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

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.

Procedure

1. Place the vCenter HA cluster in maintenance mode.
   a. In the vSphere Web 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, establish an SSH session to the Witness node.

      ```
      ssh root@Witness_node_IP_address
      ```

   b. From the appliance shell of the Witness node, 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, establish an SSH session to the Passive node.

      ```
      ssh root@Passve_node_IP_address
      ```

   b. From the appliance shell of the Passive node, 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 Web Client and click **Configure**.

   b Under **Settings**, select **vCenter HA** and click **Initiate Failover**.

   c Click **Yes** to start the failover.

      A dialog offers you the option to force a failover without synchronization. In most cases, performing synchronization first is best.

   You can see in the vSphere Web 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, establish an SSH session to the Passive node.

      ```
      ssh root@Passve_node_IP_address
      ```

   b From the appliance shell of the Passive node, 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 Web 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 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.

Troubleshooting a vSphere Upgrade 9

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.

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 screen of the GUI installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors and 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 9-1. 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.

Table 9-1. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (Continued)

Error or Warning	Description
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 does not have hardware virtualization, or if hardware virtualization is not turned on in the host BIOS, host performance suffers. You can enable hardware virtualization in the host machine boot options panel. 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 problem. To work around this problem, see Knowledge Base article KB 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. The test results indicate 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. The VMFS partition must begin after sector 1843200.
POWERPATH	This test checks for the 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 or the 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.

Table 9-1. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (Continued)

Error or Warning	Description
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 6.7 only from version 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 6.7.
UPDATE_PENDING	This test checks the host for VIB installations that require a reboot. This test fails if one or more such VIBs are installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to determine reliably which packages are currently installed on the host. If this test fails, it may 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.

Upgrade Issues with vCenter Server Containing Host Profiles

Most common issues that might occur during a vCenter Server upgrade to version 6.7, that contains host profiles.

- For issues occurring during a vCenter Server upgrade or ESXi upgrade, see *Troubleshooting a vSphere Upgrade*.
- If upgrading vCenter Server 6.0 or 6.5, containing host profiles with version earlier than 6.0, results with a failure, see KB 52932.
- For error `There is no suitable host in the inventory as reference host for the profile Host Profile. The profile does not have any associated reference host`, see KB 2150534.
- If an error occurs when you import a host profile to an empty vCenter Server inventory, see *vSphere Host Profiles* for Reference Host is Unavailable.

- If a host profile compliance check fails for NFS datastore, see *vSphere Host Profiles* for Host Profile without NFS Datastore.
- If compliance check fails with an error for the `UserVars.ESXiVPsDisabledProtocols` option, when an ESXi host upgraded to version 6.7 is attached to a host profile with version 6.0, see VMware vSphere 6.7 Release Notes.

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.

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.