vCenter Server Installation and Setup

Update 1

VMware vSphere 7.0
vCenter Server 7.0

vmware®

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

https://docs.vmware.com/

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

Contents

About vCenter Server Installation and Setup

vCenter Server Installation and Setup describes how to deploy the VMware vCenter Server® appliance.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

Intended Audience

vCenter Server Installation and Setup is for anyone who must install and configure VMware vSphere®. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Introduction to vSphere Installation and Setup

1

vSphere 7.0 provides various options for installation and setup. To ensure a successful vSphere deployment, you should understand the installation and setup options, and the sequence of tasks.

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

You deploy the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy the vCenter Server appliance on ESXi hosts or on vCenter Server instances.

For detailed information about the ESXi installation process, see *VMware ESXi Installation and Setup* .

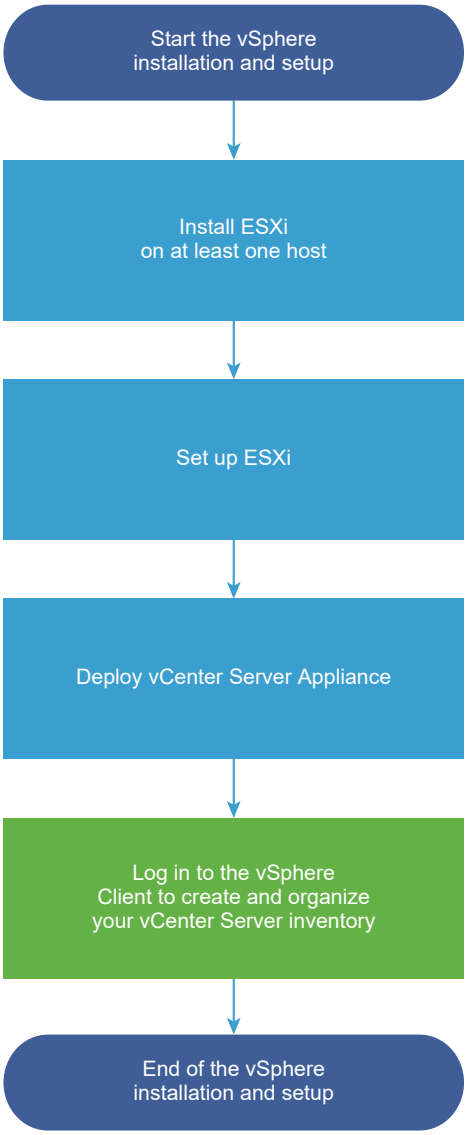
This chapter includes the following topics:

Overview of the vSphere Installation and Setup Process

vSphere is a sophisticated product with multiple components to install and set up. To ensure a successful vSphere deployment, understand the sequence of tasks required.

Installing vSphere includes the following tasks:

Figure 1-1. vSphere Installation and Setup Workflow



1 Read the vSphere release notes.

2 Install ESXi.

Note See *VMware ESXi Installation and Setup* for detailed information about the ESXi installation process.

3 Configure the ESXi boot and network settings, the direct console, and other settings. See *VMware ESXi Installation and Setup* for information.

4 Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. See *VMware ESXi Installation and Setup*.

5 Install vCenter Server.

You can deploy the vCenter Server appliance on an ESXi host or vCenter Server instance.

You can deploy or install multiple vCenter Server instances connected in Enhanced Linked Mode configuration by registering them to a common Single Sign-On domain.

a Review the topics in System Requirements for the vCenter Server Appliance and verify that your system meets the hardware and software requirements for deploying the appliance.

b Determine the deployment method to use.

You can use the GUI method to deploy the appliance interactively. Alternatively, you can use the CLI method to perform a silent deployment of the appliance. See GUI Deployment of the vCenter Server Appliance and CLI Deployment of the vCenter Server Appliance.

c Use the topic Required Information for Deploying a vCenter Server Appliance to create a worksheet with the information you need for the GUI deployment, or use the topic Prepare Your JSON Configuration File for CLI Deployment to create your JSON templates for the CLI deployment.

d Deploy the appliance.

6 Connect to vCenter Server from the vSphere Client. See Chapter 5 After You Deploy the vCenter Server Appliance.

7 Configure the vCenter Server instance. See *vCenter Server Configuration* and *vCenter Server and Host Management*.

vCenter Server Components and Services

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

When you deploy the vCenter Server appliance, vCenter Server, the vCenter Server components, and the authentication services are deployed on the same system.

The following components are included in the vCenter Server appliance deployments:

- The authentication services contain vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority.
- The vCenter Server group of services contains vCenter Server, vSphere Client, vSphere Auto Deploy, and vSphere ESXi Dump Collector. The vCenter Server appliance also contains the VMware vSphere Lifecycle Manager Extension service and the VMware vCenter Lifecycle Manager.

What Happened to the Platform Services Controller

Beginning in vSphere 7.0, deploying a new vCenter Server or upgrading to vCenter Server 7.0 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server appliance, see the *vSphere Upgrade* documentation.

Authentication Services

vCenter Single Sign-On

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

vCenter Single Sign-On is required with vCenter Server.

vSphere License Service

The vSphere License service provides common license inventory and management capabilities to all vCenter Server systems within the Single Sign-On domain.

VMware Certificate Authority

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

For information about all authentication services and capabilities, see *vSphere Authentication*.

Services Installed with vCenter Server

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

PostgreSQL

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

vSphere Client

The HTML5-based user interface that lets you connect to vCenter Server instances by using a Web browser. This vSphere Client replaces the Flex-based vSphere Web Client in vSphere 7.0.

vSphere ESXi Dump Collector

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

vSphere Auto Deploy

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

VMware vSphere Lifecycle Manager Extension

vSphere Lifecycle Manager enables centralized, automated patch and version management for VMware vSphere and offers support for VMware ESXi hosts, virtual machines, and virtual appliances. The VMware vSphere Lifecycle Manager Extension is an optional service of the vCenter Server appliance.

VMware vCenter Lifecycle Manager

The vCenter Lifecycle Manager automates the process of virtual machines and removing them from service at the appropriate time. vCenter Lifecycle Manger automatically places servers based on their location, organization, environment, service level, or performance levels. When a solution is found found for a set of criteria, the machine is automatically deployed.

Overview of the vCenter Server Appliance

The vCenter Server appliance is a preconfigured virtual machine that is optimized for running vCenter Server and the associated services.

The vCenter Server appliance package contains the following software:

- Photon OS® 3.0
- The vSphere authentication services
- PostgreSQL
- VMware vSphere Lifecycle Manager Extension
- VMware vCenter Lifecycle Manager

Version 7.0 of vCenter Server is deployed with virtual hardware version 10, which supports 64 virtual CPUs per virtual machine in ESXi.

During the deployment, you can choose the vCenter Server appliance size for your vSphere environment size and the storage size for your database requirements.

vCenter Server uses the VMware vSphere Lifecycle Manager Extension service. An external vSphere Lifecycle Manager instance on Windows is no longer required for vSphere centralized automated patch and version management. For information about the vCenter Server see vCenter Server Components and Services.

vCenter Server supports high availability. For information about configuring vCenter Server in a vCenter High Availability cluster, see *vSphere Availability*.

vCenter Server supports file-based backup and restore. For information backing up and restoring, see Chapter 3 File-Based Backup and Restore of vCenter Server.

For information about the vCenter Server maximums, see VMware Configuration Maximums.

Understanding vSphere Domains and Domain Names

Each vCenter Server is associated with a vCenter Single Sign-On domain. The domain name defaults to vsphere.local, but you can change it during deployment. The domain determines the local authentication space.

vCenter Single Sign-On Domain

When you deploy a vCenter Server appliance, you are prompted to create a vCenter Single Sign-On domain or join an existing domain.

The domain name is used by the VMware Directory Service (vmdir) for all Lightweight Directory Access Protocol (LDAP) internal structuring.

You can give your domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

After you specify the name of your domain, you can add users and groups. You can add an Active Directory or LDAP identity source and allow the users and groups in that identity source to authenticate. You can also add vCenter Server instances, or other VMware products, such as vRealize Operations, to the domain.

vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group.

You can join up to 15 vCenter Server appliance deployments with vCenter Enhanced Linked Mode in a single vSphere Single Sign-On domain.

You can create a vCenter Enhanced Linked Mode group during the deployment of vCenter Server appliance.

You can also join a vCenter Enhanced Linked Mode group by moving, or repointing, a vCenter Server from one vSphere domain to another exisitng domain. See Repoint vCenter Server to Another vCenter Server in a Different Domain for information on repointing a vCenter Server node.

vCenter Enhanced Linked Mode for vCenter Server Appliance

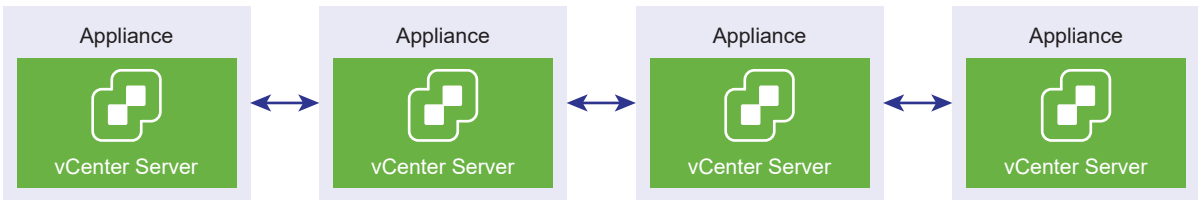
Enhanced linked mode support is enabled for vCenter Server appliance deployments.

You can connect vCenter Server appliance deployments together to form a domain.

Other features include:

- A simplified backup and restore process. See Chapter 3 File-Based Backup and Restore of vCenter Server for more information.
- A simplified HA process, removing the need for load balancers.
- Up to 15 vCenter Server appliance deployments can be linked together using enhanced linked mode and displayed in a single inventory view.
- For a vCenter High Availability (vCenter HA) cluster, three nodes are considered one logical vCenter Server node. See "vCenter Architecture Overview" in *vSphere Availability* for the vCenter HA architecture overview. A single vCenter Server standard license is needed for one vCenter HA cluster.

Figure 1-2. Enhanced Linked Mode for vCenter Server Appliance Deployments



Enhanced Linked Mode with Read Only Replication

If a vCenter High Availability (vCenter HA) instance is connected with another vCenter Server instance with enhanced linked mode and vCenter HA failover occurs to the passive node and is unable to communicate with its replication partner on the other vCenter Server node, the replica on the vCenter HA node enters read-only mode.

Joining a vCenter Enhanced Linked Mode Domain

You can join a vCenter Server appliance to another node during deployment of the vCenter Server appliance.

Note You can also join a vCenter Enhanced Linked Mode group by moving, or repointing, a vCenter Server from one vSphere domain to another exisitng domain. See Repoint vCenter Server to Another vCenter Server in a Different Domain for information on repointing a vCenter Server node.

For example, suppose you want to deploy two vCenter Server appliance systems, and join the two nodes using vCenter Enhanced Linked Mode.

If you are deploying the vCenter Server appliance nodes with the UI Installer:

1 For Appliance 1, deploy the vCenter Server appliance as an instance on ESXi Host 1. Synchronize the time settings with ESXi Host 1.

2 For Appliance 2, deploy the vCenter Server appliance as an instance on ESXi Host 1 and configure the time settings so that Appliance 2 is synchronized with ESXi Host 1. In stage 2 you select to join the vCenter Single Sign-On server of the deployed appliance on Appliance 1. For specific instructions, see Stage 2 - Set up the Newly Deployed vCenter Server Appliance.

If you are deploying the vCenter Server appliance nodes with the CLI:

1 Configure the JSON configuration template `embedded_vCSA_on_VC.json` (or `embedded_vCSA_on_ESXi.json`) for Appliance 1 as an instance on ESXi Host 1. See Prepare Your JSON Configuration File for CLI Deployment for specific instructions on preparing the JSON configuration file.

2 Deploy Appliance 1 by running the `vcsa-cli-installer` command. See Deploy a vCenter Server Appliance by Using the CLI for instructions.

3 Configure the JSON configuration template `embedded_vCSA_replication_on_VC.json` (or `embedded_vCSA_replication_on_ESXi.json`) for Appliance 2 as an instance on ESXi Host 1. Enter the hostname of the first embedded node in the `replication_partner_hostname` field in the `sso` section.

4 Deploy Appliance 2 by running the `vcsa-cli-installer` command using the `embedded_vCSA_replication_on_VC.json` (or `embedded_vCSA_replication_on_ESXi.json`) file.

Deploying the vCenter Server Appliance

2

You can deploy the vCenter Server appliance to manage your vSphere environment.

You can deploy the vCenter Server appliance on an ESXi host 6.5 or later, or on an ESXi host or DRS cluster from the inventory of a vCenter Server instance 6.5 or later.

For information about the software included in the vCenter Server appliance 7.0, see Overview of the vCenter Server Appliance.

For information about the software and hardware requirements for deploying the vCenter Server appliance, see System Requirements for the vCenter Server Appliance.

The vCenter Server installer contains executable files both for GUI and CLI deployments.

- The GUI deployment is a two stage process. The first stage is a deployment wizard that deploys the OVA file of the 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 starts the services of the newly deployed appliance.
- The CLI deployment method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that automatically deploys and sets up the appliance. The CLI deployment automatically runs both stage 1 then stage 2, with no user interaction required.

The vCenter Server appliance has the following default user names:

User Name	Description
root	Use this user name to log in to the appliance operating system and the vCenter Server Management Interface. You set the password while deploying the virtual appliance.
administrator@*your_domain_name*	Use this user name for vCenter Single Sign-On login. You set the password while creating the vCenter Single Sign-On domain. You create a vCenter Single Sign-On domain during the deployment of a vCenter Server appliance in a new vCenter Single Sign-On domain. After you create a vCenter Single Sign-On domain, only the administrator@*your_domain_name* user has the privileges required to log in to vCenter Single Sign-On and vCenter Server. The administrator@*your_domain_name* user can proceed as follows: ■ Add an identity source in which additional users and groups are defined to vCenter Single Sign-On. ■ Give permissions to the users and groups. For information about adding identity sources and giving permissions to the users and groups, see *vSphere Authentication* .

For information about upgrading and patching the vCenter Server appliance, see *vSphere Upgrade*.

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

If you want to set up vCenter Server to use an IPv6 address version, use the fully qualified domain name (FQDN) or host name of the appliance. To set up an IPv4 address, the best practice is to use the FQDN or host name of the appliance, because the IP address can change if assigned by DHCP.

This chapter includes the following topics:

System Requirements for the vCenter Server Appliance

You can deploy the vCenter Server appliance on an ESXi host 6.5 or later, or on a vCenter Server instance 6.5 or later. Your system must also meet specific software and hardware requirements.

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

Before you deploy the appliance, synchronize the clocks of the target server and all vCenter Server 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

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.

Hardware Requirements for the vCenter Server Appliance

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

Table 2-1. Hardware Requirements for a vCenter Server Appliance

	Number of vCPUs	Memory
Tiny environment (up to 10 hosts or 100 virtual machines)	2	12 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	4	19 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	8	28 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	16	37 GB
X-Large environment (up to 2,500 hosts or 45,000 virtual machines)	24	56 GB

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

Storage Requirements for the vCenter Server Appliance

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

Storage Requirements for the vCenter Server Appliance

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

Table 2-2. Storage Requirements for a vCenter Server Appliance

	Default Storage Size	Large Storage Size	X-Large Storage Size
Tiny environment (up to 10 hosts or 100 virtual machines)	415 GB	1490 GB	3245 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	480 GB	1535 GB	3295 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	700 GB	1700 GB	3460 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	1065 GB	1765 GB	3525 GB
X-Large environment (up to 2,500 hosts or 45,000 virtual machines)	1805 GB	1905 GB	3665 GB

Note The storage requirements include the requirements for the vSphere Lifecycle Manager that runs as a service in the vCenter Server appliance.

Software Requirements for the vCenter Server Appliance

The VMware vCenter Server appliance can be deployed on ESXi 6.5 hosts or later, or on vCenter Server instances 6.5 or later.

You can deploy the vCenter Server appliance 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 6.5 host on which to deploy the appliance. You can also connect to a vCenter Server 6.5 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 Installer.

Required Ports for vCenter Server

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

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

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

Table 2-3. Ports Required for Communication Between Components

Port	Protocol	Description	Used for Node-to-Node Communication
22	TCP	System port for SSHD.	No
53		DNS service	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).	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 vCenter Server.	No
389	TCP/UDP	This port must be open on the local and all remote instances of vCenter Server. This port 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.	vCenter Server to vCenter Server
443	TCP	The default port that the vCenter Server system uses to listen for connections from the vSphere Client. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. 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	vCenter Server to vCenter Server

Table 2-3. Ports Required for Communication Between Components (continued)

Port	Protocol	Description	Used for Node-to-Node Communication
514	TCP/UDP	vSphere Syslog Service port for the vCenter Server appliance.	No
636	TCP	vCenter Single Sign-On LDAPS For backward compatibility with vSphere 6.5 only.	During upgrade from vSphere 6.5 only.
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.	No
1514	TCP	vSphere Syslog Service TLS port for the vCenter Server appliance.	No
2012	TCP	Control interface RPC for vCenter Single Sign-On	No
2014	TCP	RPC port for all VMCA (VMware Certificate Authority) APIs	No
2015	TCP	DNS management	No
2020	TCP/UDP	Authentication framework management	No
5480	TCP	Appliance Management Interface Open endpoint serving all HTTPS, XMLRPS, and JSON-RPC requests over HTTPS.	No
6500	TCP/UDP	ESXi Dump Collector port	No
6501	TCP	Auto Deploy service	No
6502	TCP	Auto Deploy management	No
7080, 12721	TCP	Secure Token Service **Note** Internal ports	No
7081	TCP	vSphere Client **Note** Internal port	No
7475, 7476	TCP	VMware vSphere Authentication Proxy	No
8200, 8201, 8300, 8301	TCP	Appliance management **Note** Internal ports	No

Table 2-3. Ports Required for Communication Between Components (continued)

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

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

DNS Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance, similar to any network server, you can assign a fixed IP address and an FQDN that is resolvable by a DNS server so that clients can reliably access the service.

When you deploy the vCenter Server 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 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 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, by adding forward and reverse DNS A records.

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, 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 Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and vSphere Client.

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 2-4. Supported Guest Operating Systems and Browser Versions for the vSphere Client.

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Edge version 38 and later. Mozilla Firefox version 45 and later. Google Chrome version 50 and later.
Mac OS	Mozilla Firefox version 45 and later. Google Chrome version 50 and later.

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

Preparing for Deployment of the vCenter Server Appliance

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

The machine from which you deploy 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 Installer.

System Requirements for the vCenter Server Installer

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

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

Table 2-5. System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	■ Windows 8, 8.1, 10 ■ Windows 2012 x64 bit ■ Windows 2012 R2 x64 bit ■ Windows 2016 x64 bit ■ Windows 2019 x64	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	■ SUSE 15 ■ Ubuntu 16.04 and 18.04	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 v10.13, 10.14, 10.15 ■ macOS High Sierra, Mojave, Catalina	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 10.13 or later, 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 Installer

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

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

- Deploy the vCenter Server appliance.
- Upgrade the vCenter Server appliance.
- Converge older versions of vCenter Server with an external Platform Services Controller to the current version of vCenter Server.
- 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 installer. See System Requirements for the vCenter Server 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 the ISO image to the client machine from which you want to deploy, upgrade, migrate, or restore the appliance.

   Note ISO mounting 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 `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 is not synchronized with NTP or PTP. Similarly, issues can arise if the destination vCenter Server 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.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, 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 or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.
- When you upgrade a vCenter Server 6.5 or 6.7 instance with an external Platform Services Controller to vSphere 7.0, the upgrade process converts to a vCenter Server instance with an embedded Platform Services Controller.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

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

To learn how to change time synchronization settings for vCenter Server, see "Configure the System Time Zone and Time Synchronization Settings" in *vCenter Server Configuration*.

To learn how to edit time configuration for a host by using the vSphere Client, see "Editing Time Configuration for a Host" in *vCenter Server and Host Management*.

System Clock Synchronization Between the Client and Server

To establish a secure TLS connection to a vCenter Server (the server), the system where you are running the CLI installer (the client) must not have its system clock slower or faster than the server's system clock by an acceptable limit (tolerance).

See Table 2-6. Client Clock Tolerance for specific values for each deployment scenario.

Note The client clock values are applicable only for vCenter Server 6.7 and later.

Table 2-6. Client Clock Tolerance

Deployment Scenario	Clock Tolerance	Connection Notes
Linking one vCenter Server with another vCenter Server	When deploying the second vCenter Server, the clock tolerance for the client and the first vCenter Server must not exceed 10 minutes.	
Installing a vCenter Server appliance using a container vCenter Server with a `*._on_vc.json` template.	The maximum clock tolerance between the client and the container vCenter Server is 8 hours 20 minutes.	

Prerequisites for Deploying the vCenter Server Appliance

To ensure a successful deployment of the vCenter Server appliance, you must perform some required tasks and pre-checks before running the installer.

General Prerequisites

- Download and Mount the vCenter Server Installer.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the vCenter Server Appliance.
- If you want to deploy the appliance on an ESXi host, verify that the ESXi host is not in lockdown or maintenance mode and not part of a fully automated DRS cluster.
- If you want to deploy the 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 use NTP servers for time synchronization, verify that the NTP servers are running and that the time between the NTP servers and the target server on which you want to deploy the appliance is synchronized.

vCenter Enhanced Linked Mode Prerequisites

When deploying a new vCenter Server as part of an Enhanced Linked Mode deployment, create an image-based backup of the existing vCenter Server nodes in your environment. You can use the backup as a precaution in case there is a failure during the deployment process.

If the deployment fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server nodes from their respective image-based backups. You must restore all the nodes in the environment from their image-based backups. Failing to do so can cause the replication partners to be out of synchronization with the restored node.

- To learn more about creating vCenter Enhanced Linked Mode deployments, see vCenter Enhanced Linked Mode.

- To learn about image-based backs, see Chapter 4 Image-Based Backup and Restore of a vCenter Server Environment.

Network Prerequisites

If you plan to assign a static IP address and an FQDN as a system name in the network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.

GUI Deployment of the vCenter Server Appliance

You can use the GUI installer to perform an interactive deployment of a vCenter Server appliance.

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

The GUI deployment process includes a series of two stages.

Figure 2-1. Stage 1 - OVA Deployment

The first stage walks you through the deployment wizard to choose the deployment type and appliance settings. This stage completes the deployment of the OVA file on the target server with the deployment type and appliance settings that you provide.

As an alternative to performing the first stage of the deployment with the GUI installer, you can deploy the OVA file of the vCenter Server appliance by using the vSphere Client. After the OVA deployment, you must log in to the vCenter Server Management Interface of the newly deployed appliance to proceed with the second stage of the deployment process. See "Deploy an OVF or OVA Template" in *vSphere Virtual Machine Administration* vSphere Virtual Machine Administration for information about deploying an OVA file using the vSphere Client.

Figure 2-2. Stage 2 - Appliance Setup

The second stage walks you through the setup wizard to configure the appliance time synchronization and vCenter Single Sign-On. This stage completes the initial setup and starts the services of the newly deployed appliance.

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

Required Information for Deploying a vCenter Server Appliance

When you use the GUI method to deploy a vCenter Server appliance, the wizard prompts you for deployment and setup information. It is a best practice to keep a record of the values that you enter in case you must reinstall the product.

You can use this worksheet to record the information that you need for deploying a vCenter Server appliance.

Table 2-7. Required Information During Stage 1 of the GUI Deployment Process

Required Information	Default	Your Entry
FQDN or IP address of the target server on which you want to deploy the appliance. The target server can be either an ESXi host or a vCenter Server instance.	-	
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	-	
Data center from the vCenter Server inventory on which you want to deploy the appliance . Target server must be a vCenter Server instance. 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 appliance	-	
VM name for the appliance ■ Must not contain a percent sign (%), backslash (\), or forward slash (/) ■ Must be no more than 80 characters in length	vCenter Server	

Table 2-7. Required Information During Stage 1 of the GUI Deployment Process (continued)

Required Information	Default	Your Entry
Password for the root user of the appliance operating system ■ Must contain only lower ASCII characters without spaces. ■ Must be at least 8 characters, but no more than 20 characters in length ■ Must contain at least one uppercase letter ■ Must contain at least one lowercase letter ■ Must contain at least one number ■ Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!)	-	
Deployment size of the vCenter Server appliance for your vSphere environment ■ Tiny Deploys an appliance with 2 CPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines. ■ Small Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines. ■ Medium Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines. ■ Large Deploys an appliance with 16 CPUs and 37 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 56 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines.	Tiny	

Table 2-7. Required Information During Stage 1 of the GUI Deployment Process (continued)

Required Information	Default	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 415 GB of storage. For small deployment size, deploys the appliance with 480 GB of storage. For medium deployment size, deploys the appliance with 700 GB of storage. For large deployment size, deploys the appliance with 1065 GB of storage. For x-large deployment size, deploys the appliance with 1805 GB of storage. ■ Large For tiny deployment size, deploys the appliance with 1490 GB of storage. For small deployment size, deploys the appliance with 1535 GB of storage. For medium deployment size, deploys the appliance with 1700 GB of storage. For large deployment size, deploys the appliance with 1765 GB of storage. For x-large deployment size, deploys the appliance with 1905 GB of storage. ■ X-Large For tiny deployment size, deploys the appliance with 3245 GB of storage. For small deployment size, deploys the appliance with 3295 GB of storage. For medium deployment size, deploys the appliance with 3460 GB of storage. For large deployment size, deploys the appliance with 3525 GB of storage. For x-large deployment size, deploys the appliance with 3665 GB of storage.	Default	

Table 2-7. Required Information During Stage 1 of the GUI Deployment Process (continued)

Required Information	Default	Your Entry
Name of the datastore on which you want to store the configuration files and virtual disks of the appliance **Note** The installer displays a list of datastores that are accessible from your target server.	-	
Enable or disable Thin Disk Mode	Disabled	
Name of the network to which to connect the 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 client machine from which you perform the deployment.	-	
IP version for the appliance address Can be either IPv4 or IPv6.	IPv4	
IP assignment for the appliance address Can be either static or DHCP.	static	
FQDN For a static IP assignment vCenter Server uses FQDN or IP address as the system name.	-	
IP address	-	
For IPv4 networks, you can use either a subnet mask or a network prefix. Subnet mask uses a dot decimal notation (for example, 255.255.255.0). An IPv4 network prefix is an integer between 0 and 32. For IPv6 networks, you must use a network prefix. An IPv6 network prefix is an integer between 0 and 128 .	-	
Default gateway	-	
DNS servers separated by commas	-	
System name (FQDN) For a DHCP assignment with IPv4 version and a DDNS server is available in your environment.	-	

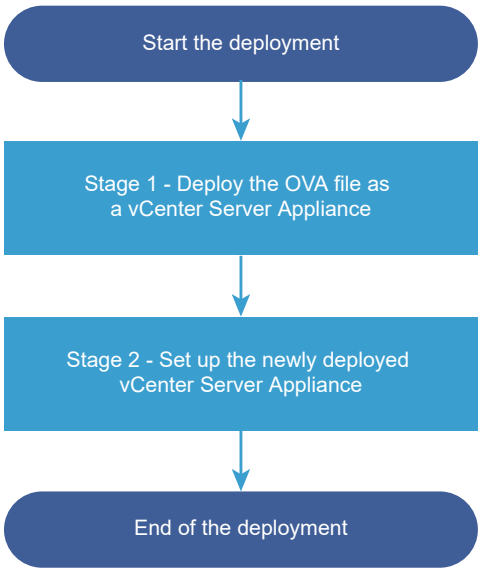
Table 2-8. Required Information During Stage 2 of the GUI Deployment Process

Required Information	Default	Your Entry
Time synchronization settings You can synchronize the time of the appliance either with the time of the ESXi host or with one or more NTP servers. If you want to use more than one NTP servers, you must provide the IP addresses or FQDNs of the NTP servers as a comma-separated list.	Synchronize time with NTP servers	
Enable or disable SSH access **Note** vCenter Server High Availability requires remote SSH access to the appliance.	Disabled	
Name for the new vCenter Single Sign-On domain For example, vsphere.local.	-	
Password for the administrator account, administrator@*your_domain_name* ■ 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, such as ampersand (&), hash key (#), and percent sign (%)	-	
Password of the vCenter Single Sign On administrator user for the domain	-	
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	

Deploy the vCenter Server Appliance by Using the GUI

You can use the GUI installer to perform an interactive deployment of a vCenter Server appliance. You must run the GUI deployment from a Windows, Linux, or Mac machine that is in the network on which you want to deploy the appliance.

Figure 2-3. Deployment Workflow of a vCenter Server Appliance



Prerequisites

- See Prerequisites for Deploying the vCenter Server Appliance.
- See Required Information for Deploying a vCenter Server Appliance.

Procedure

1 Stage 1 - Deploy the OVA File as a vCenter Server Appliance

With stage 1 of the deployment process, you deploy the OVA file, which is included in the vCenter Server installer, as a vCenter Server appliance.

2 Stage 2 - Set up the Newly Deployed vCenter Server Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the deployment process to set up and start the services of the newly deployed vCenter Server appliance.

Stage 1 - Deploy the OVA File as a vCenter Server Appliance

With stage 1 of the deployment process, you deploy the OVA file, which is included in the vCenter Server installer, as a vCenter Server appliance.

Procedure

1 In the vCenter Server 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 **Install** to start the deployment wizard.

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

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

5 Connect to the target server on which you want to deploy the vCenter Server appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the 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 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target ESXi host, and click **Yes** to accept the certificate thumbprint.
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 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 user with vCenter Single Sign-On administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target vCenter Server instance, and click **Yes** to accept the certificate thumbprint. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the 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 appliance, and click **Next**.

6 On the Set up appliance VM page, enter a name for the 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 (()).

7 Select the deployment size for the vCenter Server appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines

Deployment Size Option	Description
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 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 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

8 Select the storage size for the 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 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

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 On the Configure network settings page, set up the network settings.

The IP address or the FQDN of the appliance is used as a system name. It is recommended to use an FQDN. However, if you want to use an IP address, use static IP address allocation for the appliance, because IP addresses allocated by DHCP might change.

Option	Action
Network	Select the network to which to connect the appliance. 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 not supported and are not displayed in the drop-down menu.
IP version	Select the version for the appliance IP address. You can select either IPv4 or IPv6.

Option	Action
IP assignment	Select how to allocate the IP address of the appliance. ■ **static** The wizard prompts you to enter the IP address and network settings. ■ **DHCP** A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment. If there is an enabled DDNS in your environment, you can enter a preferred fully qualified domain name (FQDN) for the appliance.
Common Ports	You can customize the HTTP and HTTPS ports (optional). If specifying a custom HTTP and HTTPS port number, ensure that you do not use a port number already in use by vCenter Server, or the default HTTP and HTTPS ports of 80 and 443.

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

12 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 Management Interface to set up and start the services.

Results

The newly deployed vCenter Server appliance is running on the target server but the services are not started.

Stage 2 - Set up the Newly Deployed vCenter Server Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the deployment process to set up and start the services of the newly deployed vCenter Server appliance.

Procedure

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

2 Configure the time settings in the appliance, optionally enable remote SSH access to the appliance, and click **Next**.

Option	Description
Synchronize time with the ESXi host	Enables periodic time synchronization, and VMware Tools sets the time of the guest operating system to be the same as the time of the ESXi host.
Synchronize time with NTP servers	Uses a Network Time Protocol server for synchronizing the time. If you select this option, you must enter the names or IP addresses of the NTP servers separated by commas.

3 Create a new vCenter Single Sign-On domain or join an existing domain.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On domain. a Enter the domain name, for example **vsphere.local**. b Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*your_domain_name*. c Confirm the administrator password, and click **Next**.
Join an existing vCenter Single Sign-On domain	Joins a new vCenter Single Sign-On server to an existing vCenter Single Sign-On domain. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. a Enter the fully qualified domain name (FQDN) or IP address of the vCenter Single Sign-On server to join. b Enter the HTTPS port to use for communication with the vCenter Single Sign-On server. c Enter the domain name for the vCenter Single Sign-On you are joining, for example **vsphere.local**. d Enter the password of the vCenter Single Sign-On administrator account. e Click **Next**.

When you select to join an existing vCenter Single Sign-On domain, you enable the Enhanced Linked Mode feature. The infrastructure data is replicated with the joined vCenter Single Sign-On server.

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 configuration settings for the vCenter Server appliance, click **Finish**, and click **OK** to complete stage 2 of the deployment process and set up the appliance.

6 (Optional) After the initial setup finishes, enter the URL from the browser with **https://*vcenter_server_appliance_fqdn*/ui** to go to the vSphere Client and log in to the vCenter Server instance in the vCenter Server appliance, or click the **https://*vcenter_server_appliance_fqdn*:443** to go the vCenter Server appliance Getting Started page.

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

You are redirected to the vCenter Server appliance Getting Started page.

What to do next

You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

CLI Deployment of the vCenter Server Appliance

You can use the CLI installer to perform a silent deployment of a vCenter Server appliance on an ESXi host or vCenter Server instance.

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

The vCenter Server appliance ISO file contains templates of JSON files that contain the minimum configuration parameters that are required for deploying the vCenter Server appliance. For information about preparing JSON templates for CLI deployment, see Prepare Your JSON Configuration File for CLI Deployment.

Deploy a vCenter Server Appliance by Using the CLI

You can use the CLI installer to perform an unattended deployment of a vCenter Server appliance. You must run the CLI deployment from a Windows, Linux, or Mac machine that is in the network on which you want to deploy the appliance.

Prerequisites

- See Prerequisites for Deploying the vCenter Server Appliance.
- Prepare Your JSON Configuration File for CLI Deployment.
- Review Syntax of the CLI Deployment Command.
- Verify that the user name with which you are logged in to your client machine, the path to the vCenter Server 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.
- The Visual C++ redistributable libraries version 14.0 or newer needs to be installed to run this utility on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa\ovftool\win32\vcredist` directory.

Procedure

1. Navigate to the `vcsa-cli-installer` subdirectory for your operating system.
   - If you are running the deployment on Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are running the deployment on Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.

- If you are running the deployment on Mac OS, navigate to the `vcsa-cli-installer/mac` directory.

2 (Optional) Run a pre-deployment check without deploying the appliance to verify that you prepared the deployment template correctly.

```
vcsa-deploy install --precheck-only path_to_the_json_file
```

3 Run the deployment command.

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

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

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

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

Prepare Your JSON Configuration File for CLI Deployment

Before you run the CLI installer to deploy a vCenter Server appliance, you must prepare a JSON file with configuration parameters and their values for your deployment specification.

The vCenter Server installer contains JSON templates for all deployment options. For information about the templates, see JSON Templates for CLI Deployment of the vCenter Server Appliance.

You can deploy 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 install --template-help` command or see Deployment Configuration Parameters.

Prerequisites

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

Procedure

1 In the vCenter Server installer, navigate to the `vcsa-cli-installer` directory, and open the `templates` subfolder.

2 Copy the deployment templates from the `install` 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 In a text editor, open the template file for your specification.

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 network of the appliance, in the `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.

```
"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-7.0.0.XXXX-YYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYY_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 deployment specification.

JSON Templates for CLI Deployment of the vCenter Server Appliance

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

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

Table 2-9. Deployment JSON Templates Included in the vCenter Server Installer

Location	Template	Description
vcsa-cli-installer\templates\install	embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server appliance on an ESXi host.
	embedded_vCSA_on_VC.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server appliance on a vCenter Server instance.
	embedded_vCSA_replication_on_ESXi.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server appliance as a replication partner to another embedded vCenter Server on an ESXi host.
	embedded_vCSA_replication_on_VC.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server appliance replication partner to another vCenter Server appliance on a vCenter Server instance.

Deployment Configuration Parameters

When you prepare your JSON configuration files for CLI deployment, you must set parameters and values to provide input data for the deployment of a vCenter Server appliance.

Sections and Subsections of Configuration Parameters in the JSON Deployment Files

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

Table 2-10. Sections and Subsections of Configuration Parameters in the JSON Deployment Files

Section	Subsection	Description
new_vcsa - describes the appliance that you want to deploy	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. See Table 2-11. Configuration Parameters in the new_vcsa Section, esxi Subsection. **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. See Table 2-12. Configuration Parameters in the new_vcsa Section, vc Subsection. **Note** You must fill in either the vc or the esxi subsection.

Table 2-10. Sections and Subsections of Configuration Parameters in the JSON Deployment Files (continued)

Section	Subsection	Description
	`appliance`	Contains the configuration parameters that describe the appliance. See Table 2-13. Configuration Parameters in the new_vcsa Section, appliance Subsection.
	`network`	Contains the configuration parameters that describe the network settings for the appliance. See Table 2-14. Configuration Parameters in the new_vcsa Section, network Subsection.
	`os`	Contains the configuration parameters that describe the operating system settings for the appliance. See Table 2-15. Configuration Parameters in the new_vcsa Section, os Subsection.
	`sso`	Contains the configuration parameters that describe the vCenter Single Sign-On settings for the appliance. See Table 2-16. Configuration Parameters in the new_vcsa Section, sso Subsection.
	`ovftool_arguments`	Optional subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates. **Important** The vCenter Server 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.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP)	`settings`	Contains only the `ceip_enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). See Table 2-17. Configuration Parameters in the ceip Section, settings Subsection. **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*.

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-7.0.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYYY_OVF10.ova`.

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

Configuration Parameters in the new_vcsa Section

Table 2-11. 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 to deploy the appliance.
username	string	A user name with administrative privileges on the target ESXi host, for example, root.
password	string	The password of the user with administrative privileges on the target ESXi host.
deployment_network	string	The name of the network to which to connect the appliance. **Note** The network must be accessible from the target ESXi host. Ignored if the target ESXi host has only one network.
datastore	string	The name of the datastore where you want to store the configuration files and virtual disks of the appliance. **Note** The datastore must be accessible from the ESXi host. If you are using the thin disk mode, the datastore size should have a miniumu of 25GB space.
port	integer	The HTTPS reverse proxy port of the target ESXi host. The default port is 443. Use only if the target ESXi host uses a custom HTTPS reverse proxy port.

Table 2-12. 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 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 2-12. 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 appliance.
		If the datacenter is located in a folder or a structure of folders, the value must be either a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "datacenter_name"]`
		or
		`"parent_folder, child_folder, datacenter_name"`
		Note The value is case-sensitive.

`datastore`	string	The name of the datastore that you want to store the 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 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.

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

`vm_folder`	string	Optional. The name of the VM folder where the appliance is deployed.

Table 2-13. 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 for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 315 GB of storage. ■ Set to `tiny-lstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 1390 GB of storage. ■ Set to `tiny-xlstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 3145 GB of storage. ■ Set to `small` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 380 GB of storage. ■ Set to `small-lstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 1435 GB of storage. ■ Set to `small-xlstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 3195 GB of storage. ■ Set to `medium` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 600 GB of storage. ■ Set to `medium-lstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 1600 GB of storage. ■ Set to `medium-xlstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 3360 GB of storage. ■ Set to `large` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 37 GB of memory, and 965 GB of storage. ■ Set to `large-lstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the large storage size.

Table 2-13. Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection (continued)

Name	Type	Description
		Deploys an appliance with 16 CPUs, 37 GB of memory, and 1665 GB of storage. ■ Set to `large-xlstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 37 GB of memory, and 3425 GB of storage. ■ Set to `xlarge` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 1705 GB of storage. ■ Set to `xlarge-lstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 1805 GB of storage. ■ Set to `xlarge-xlstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 3565 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server appliance installation package. By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool_path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 2-14. Configuration Parameters in the `new_vcsa` Section, `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 2-14. Configuration Parameters in the `new_vcsa` Section, `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"`
		Optional when the `mode` parameter is set to `static`. Not supported when mode is set to `DHCP`.

`prefix`	string	Network prefix length. 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 IPv6 version, the value can be `default`.
`ports`	string	Optional. Port numbers that the vCenter Server appliance uses for direct HTTP connections. By default, port 80 redirects requests to HTTPS port 443. You can customize the vCenter Server HTTP and HTTPS ports. If specifying a custom HTTP and HTTPS port number, ensure that you do not use a port already in use by vCenter Server, or the default HTTP and HTTPS ports of 80 and 443. The options to specify a custom port are: `"rhttpproxy.ext.port1":"`*`port_number`*`"` for the HTTP port, and `"rhttpproxy.ext.port2:"`*`port_number`*`"` for the HTTPS port. The following example specifies ports 81 and 444 for the HTTP and HTTPS ports: `ports: {"rhttpproxy.ext.port1":"81", "rhttpproxy.ext.port2":"444"}` For more information on ports in use by vCenter Server, see Required Ports for vCenter Server .
`system_name`	string	Primary network identity. Can be an IP address or FQDN, preferably FQDN. You cannot change the value of this parameter after the deployment. The FQDN and dotted-decimal numbers must comply with the RFC 1123 guidelines.

Table 2-15. 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.

ntp_servers	string or array	Optional. Host names or IP addresses of one or more NTP servers for time synchronization.
		To set more than one NTP 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"`

ssh_enable	Boolean	Set to true to enable SSH administrator login to the appliance. **Note** vCenter Server appliance high availability requires remote SSH access to the appliance.
time_tools_sync	Boolean	Optional. Set to true to deploy the appliance with the VMware Tools time synchronization. VMware Tools synchronizes the time of the appliance with the time of the ESxi host. Ignored if you set NTP servers for time synchronization, that is, if you set the ntp.servers parameter.

Table 2-16. Configuration Parameters in the new_vcsa Section, sso Subsection

Name	Type	Description
password	string	Password of the vCenter Single Sign-On administrator user, administrator@*your_domain_name*. If you are deploying a vCenter Server appliance as the first instance in a new vCenter Single Sign-On domain, you must set the password for the vCenter Single Sign-On administrator user. 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 ASCII characters.
domain_name	string	vCenter Single Sign-On domain name, for example, vsphere.local. If you are deploying a vCenter Server appliance as the first instance in a new vCenter Single Sign-On domain, you must set the name for the new vCenter Single Sign-On domain.

Table 2-16. Configuration Parameters in the `new_vcsa` Section, `sso` Subsection (continued)

Name	Type	Description
`replication_partner_hostname`	string	The system name of the partner vCenter Server. Required only if you are deploying a replication partner in an existing vCenter Single Sign-On domain.
`sso_port`	integer	The HTTPS reverse proxy port of the partner vCenter Server . The default port is 443. Use only if the partner uses a custom HTTPS reverse proxy port.

Configuration Parameters in the `ceip` Section

Table 2-17. Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
`ceip_enabled`	Boolean	Set to `true` to join the CEIP for this appliance.

Syntax of the CLI Deployment Command

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

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

```
vcsa-deploy install path_to_the_json_file list_of_arguments
```

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

Argument	Description
`--operation-id` *OPERATION_ID*	Provides an operation ID to track installation activities.
`--pause-on-warnings`	Pauses and waits for acknowledgment of warnings.
`--verify-template-only`	Performs basic template verification of the configuration parameters in the JSON file. Does not deploy the appliance.
`--precheck-only`	Performs only the basic template verification and OVF Tool parameter verification. Does not deploy the appliance.
`--sso-ssl-thumbprint` *SSL-SHA1-THUMBPRINT*	Validates server certificate against the supplied SHA1 thumbprint.
`-h`, `--help`	Displays the help message for the `vcsa-deploy install` command.
`--template-help`	Displays the help message for the use of configuration parameters in the JSON deployment 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

Deploy Multiple vCenter Server Appliances Using the CLI

You can deploy multiple instances vCenter Server appliances concurrently (in batch mode) using the CLI installer.

To deploy multiple instances concurrently, create JSON templates for all the vCenter Server instances in your deployment. The CLI installer assesses the topology of the deployment using the JSON templates, and determines the order. For this reason, the JSON templates must use static IP addresses for all vCenter Server instances in the deployment that are dependant upon one another.

Important The JSON templates you create for each appliance must use a static IP address to resolve the network addresses of other appliances in the deployment upon which they have a dependency.

To perform the batch deployment, place the JSON templates defining your deployment in a single directory. When invoked, the CLI installer deploys your existing deployment using the topology defined in the JSON templates.

Procedure

1 In your workspace, create a folder to contain the JSON files for batch deployment. For example, *MyWorkspace*`/BatchDeploy`.

2 Prepare each JSON configuration file and copy the file to your batch deployment folder. See Prepare Your JSON Configuration File for CLI Deployment for instructions on configuring the JSON files.

3 Navigate to the `vcsa-cli-installer` subdirectory for your operating system.

- If you are running the deployment on Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
- If you are running the deployment on Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
- If you are running the deployment on Mac OS, navigate to the `vcsa-cli-installer/mac` directory.

4 (Optional) Run a pre-deployment check without deploying the appliance to verify that you prepared the deployment template correctly. For example:

```
vcsa-deploy install --precheck-only MyWorkspace/BatchDeploy
```

5 Run the deployment command. For example,

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments MyWorkspace/BatchDeploy
```

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

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

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location MyWorkspace/
BatchDeploy
```

File-Based Backup and Restore of vCenter Server

3

vCenter Server supports a file-based backup and restore mechanism that helps you to recover your environment after failures.

You can use the vCenter Server Interface to create a file-based backup of the vCenter Server. After you create the backup, you can restore it by using the GUI installer of the appliance.

You use the vCenter Server Interface to perform a file-based backup of the vCenter Server core configuration, inventory, and historical data of your choice. The backed-up data is streamed over FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB to a remote system. The backup is not stored on the vCenter Server.

You can perform a file-based restore only for a vCenter Server that you have previously backed up by using the vCenter Server Interface. You can perform such restore operation by using the GUI installer of the vCenter Server appliance. The process consists of deploying a new vCenter Server appliance and copying the data from the file-based backup to the new appliance.

You can also perform a restore operation by deploying a new vCenter Server appliance and using the vCenter Server Interface to copy the data from the file-based backup to the new appliance.

Important If you back up a vCenter Server High Availability cluster, the backup operation only backs up the primary vCenter Server instance. Before restoring a vCenter Server High Availability cluster, you must power off the active, passive, and witness nodes. The restore operation restores the vCenter Server in non-vCenter Server High Availability mode. You must reconstruct the cluster after the restore operation completes successfully.

This chapter includes the following topics:

Considerations and Limitations for File-Based Backup and Restore

When you backup or restore a vCenter Server environment, take into account these considerations and limitation.

Protocols

The following considerations apply to file-based backup and restore protocols:

- FTP and HTTP are not secure protocols
- Backup servers must support minimum of 10 simultaneous connections for each vCenter Server
- You must have write permissions for upload and read permissions for download
- Only explicit mode is supported for FTPS
- If you use HTTP or HTTPS, you must enable WebDAV on the backup Web server
- You can use only FTP, FTPS, HTTP, or HTTPS to transmit data through an HTTP proxy server
- You can use IPv4 and IPv6 URLs in file-based backup and restore of a vCenter Server. Mixed mode of IP versions between the backup server and the vCenter Server is unsupported.
- The vCenter Server appliance GUI installer does not support restore from a backup with NFS or SMB protocol. To perform a restore from an NFS or SMB protocol, use the vCenter Server Management API.

Configuration

After a restore, the following configurations revert to the state when the backup was taken.

- Virtual machine resource settings
- Resource pool hierarchy and setting
- Cluster-host membership
- DRS configuration and rules

Storage DRS

If the configuration changes, the following might change after a restore.

- Datastore Cluster configuration
- Datastore Cluster membership
- Datastore I/O Resource Management (Storage I/O Control) settings
- Datastore-Datacenter membership
- Host-Datastore membership

Distributed Power Management

If you put a host into standby mode after a backup, the vCenter Server might force the host to exit standby mode when you restore to the backup.

Distributed Virtual Switch

If you use a distributed virtual switch, you are advised to export separately the distributed virtual switch configuration before you restore to a backup. You can import the configuration after the restore. If you omit this consideration, you may lose the changes made to a distributed virtual switch after the backup. For detailed steps, see the VMware knowledge base article at http://kb.vmware.com/kb/2034602.

Content Libraries

If you delete libraries or items after a backup, you cannot access or use these libraries or items after the restore. You can only delete such libraries or items. A warning message notifies you that there are missing files or folders in the storage backup.

If you create new items or item files after the backup, the Content Library Service has no record of the new items or files after the restore operation. A warning notifies you that extra folders or files were found on the storage backup.

If you create new libraries after the backup, the Content Library Service has no record of the new libraries after restore. The library content exists on the storage backing, but no warning is displayed. You must manually clean the new libraries.

Virtual Machine Life Cycle Operations

- Restoring vCenter Server from a backup that was taken during in-flight relocation operations in the vCenter Server instance.

  After you restore vCenter Server, the vCenter Server view of the virtual machines might be out of sync with the ESXi view of the virtual machines. This is also true if you performed the backup during in-flight operations on vCenter Server. If virtual machines disappear after you restore vCenter Server, you can refer to the following cases.

  a The missing virtual machine is located on the destination ESXi host and is registered with the destination ESXi host, but it is either an orphan or not in the vCenter Server inventory. You must manually add the virtual machine to the vCenter Server inventory.

  b The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host and it is not in the vCenter Server inventory. You must manually register the virtual machine to the ESXi host and add the virtual machine back to the vCenter Server inventory.

  c The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host. In the vCenter Server instance, the missing virtual machine is marked as orphaned. You must remove the virtual machine from the vCenter Server inventory and add it again.

- Restoring vCenter Server from a backup that has an out-of-date linked clone virtual machine layout.

  If you create a linked clone virtual machine after the backup and you restore vCenter Server from the old backup, then after the restore, the vCenter Server does not know about the new linked clone virtual machine until vCenter Server discovers the new linked clone virtual machine. If you remove all existing virtual machines before the new linked clone virtual machine is discovered, then the removal of existing virtual machines corrupts the new linked clone due to missing disks. In order to avoid this, you must wait until all linked clone virtual machines are discovered by the vCenter Server before you remove virtual machines.

- Restoring vCenter Server from a backup that was taken during virtual machine registration.

  If you are registering a virtual machine during the backup and you restore vCenter Server from the old backup, then after the restore, the virtual machine is marked as orphaned in the vCenter Server instance. You must manually add the virtual machine to the vCenter Server inventory.

vSphere High Availability

Restoring vCenter Server from a backup might cause it to rollback to older version for the vSphere HA cluster state (HostList, ClusterConfiguration, VM protection state) while the hosts in the cluster have the latest version for the cluster state. You need to make sure the vSphere HA cluster state stays the same during restore and backup operations. Otherwise, the following problems might occur.

- If hosts are added or removed to or from the vSphere HA cluster after backup and before vCenter Server restore, virtual machines could potentially failover to hosts not being managed by the vCenter Server but are still part of the HA cluster.
- Protection state for new virtual machines is not updated on the vSphere HA agents on the hosts that are part of the vSphere HA cluster. As a result, virtual machines are not protected or unprotected.
- New cluster configuration state is not updated on the vSphere HA agents on the hosts that are part of the vSphere HA cluster.

vCenter High Availability

Restoring vCenter Server requires vCenter HA to be reconfigured.

Storage Policy Based Management

Restoring vCenter Server from a backup can lead to the following inconsistencies related to storage policies, storage providers, and virtual machines.

- Registered storage providers after backup are lost.
- Unregistered storage providers after backup re-appear and might show different provider status.

- Changes, such as create, delete, or update, performed on storage policies after backup are lost.
- Changes, such as create, delete, or update, performed on storage policy components after backup are lost.
- Default policy configuration changes for datastores performed after backup are lost.
- Changes in the storage policy association of the virtual machine and its disks, and in their policy compliance might occur.

Virtual Storage Area Network

Restoring vCenter Server from a backup might cause inconsistencies in the vSAN. For information on how to check vSAN health, see *Administering VMware vSAN*.

Patching

Restoring vCenter Server from a backup might result in missing security patches. You must apply them again after the restore is complete. For information on patching the vCenter Server, see *vSphere Upgrade*.

Schedule a File-Based Backup

You can schedule file-based backups for vSphere 6.7 and later. You can set up a schedule that is used to perform periodic backups.

The schedule can be set up with information about the backup location, recurrence, and retention for the backups.

You can only set up one schedule at a time.

Prerequisites

- You must have a FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server up and running with sufficient disk space to store the backup.

Procedure

1. In a Web browser, go to the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
2. Log in as root.
3. In the vCenter Server Management Interface, click **Backup**.
4. Click **Configure** to set up a backup schedule.

5 Enter the backup location details.

Option	Description
Backup location	Enter the backup location, including the protocol to use to connect to your backup server, the port, the server address, and backup folder to store the backup files. Use one of the following protocols: FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB. For FTP, FTPS, HTTP, or HTTPS the path is relative to the home directory configured for the service.
Backup server credentials	Enter a user name and password of a user with **write** privileges on the backup server.

6 Set the schedule recurrence and time for the backup.

The recurrence can be set daily, weekly, or you can customize the schedule to run the backup on a specific day or days of the week. You can specify the time of day to run the backup. The default time is 11:59pm.

7 (Optional) Enter an Encryption Password if you want to encrypt your backup file.

If you select to encrypt the backup data, you must use the encryption password for the restore procedure.

8 Select **Retain all backups** or enter the number of backups to retain.

The retention information provides the number of backups to retain for a given vCenter Server.

9 (Optional) Select **Stats, Events, and Tasks** to back up additional historical data from the database.

10 Click **Create**.

The backup schedule information is populated in the Backup page.

Results

The complete and in progress backups are listed under Activity.

What to do next

You can perform an immediate backup with the existing schedule information by selecting **Use backup location and user name from backup schedule** from the backup schedule on the Backup Now dialog box.

Manually Back up vCenter Server by Using the vCenter Server Management Interface

You can use the vCenter Server Management Interface to back up the vCenter Server instance. You can select whether to include historical data, such as stats, events, and tasks, in the backup file.

Note The backup operation for a vCenter High Availability cluster, backs up only the active node.

Prerequisites

- You must have an FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server up and running with sufficient disk space to store the backup.

Procedure

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

   The table under Activity displays the most current backup version taken of the vCenter Server.
4. Click **Backup Now**.

   The **Backup Appliance** wizard opens.
5. (Optional) Select **Use backup location and user name from backup schedule** to use the information from a scheduled backup.
6. Enter the backup location details.

Option	Description
Backup location	Enter the backup location, including the protocol to use to connect to your backup server, the port, the server address, and backup folder to store the backup files. Use one of the following protocols: FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB. For FTP, FTPS, HTTP, or HTTPS the path is relative to the home directory configured for the service.
Backup server credentials	Enter a user name and password of a user with **write** privileges on the backup server. **Note** Username and password should only contain ASCII characters.

7 (Optional) Enter an Encryption Password if you want to encrypt your backup file.

   If you select to encrypt the backup data, you must use the encryption password for the restore procedure.

8 (Optional) Select **Stats, Events, and Tasks** to back up additional historical data from the database.

9 (Optional) In the **Description** text box, enter a description of the backup.

10 Click **Start** to begin the backup process.

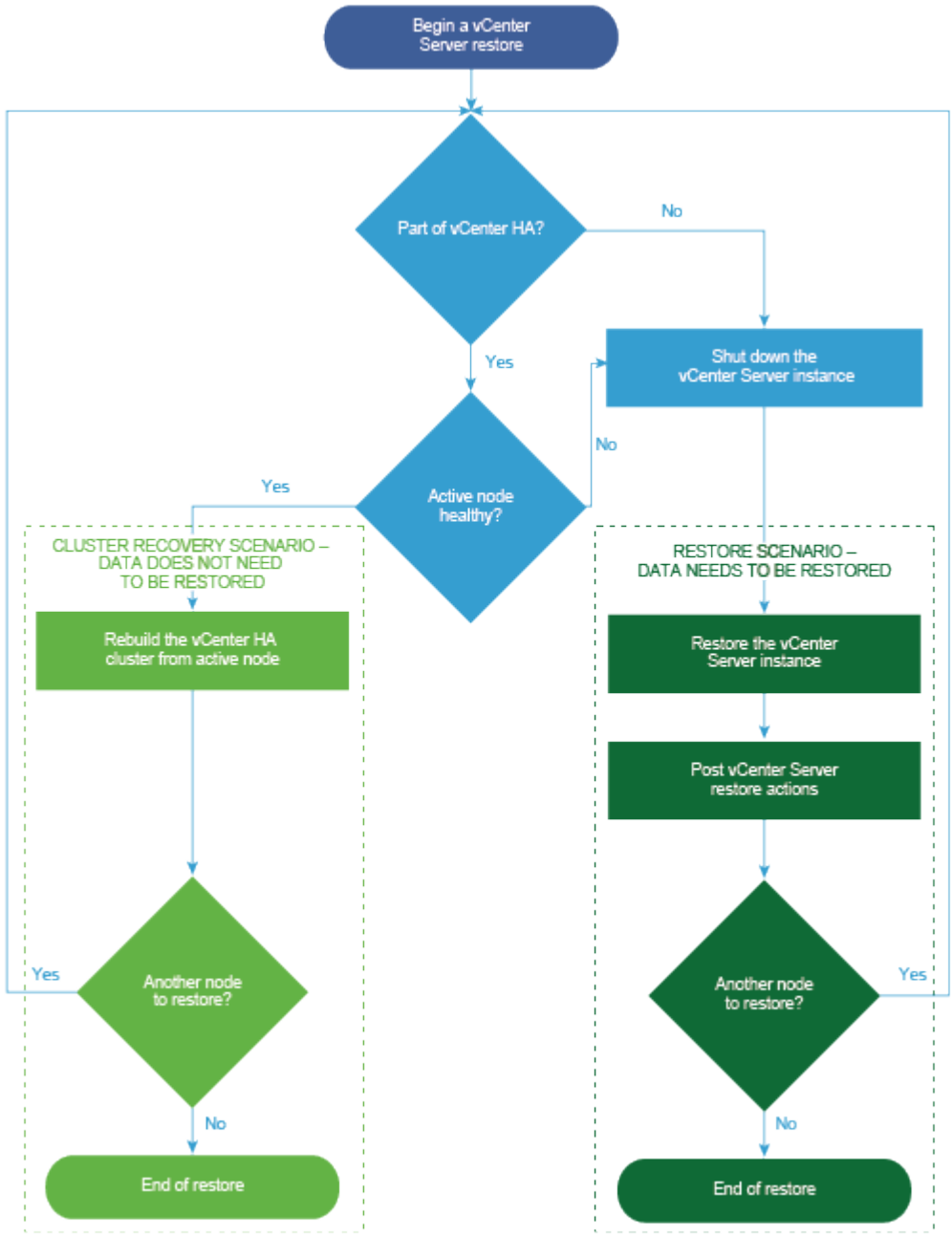
Results

The complete and in progress backups are listed under Activity.

Restore vCenter Server from a File-Based Backup

You can use the vCenter Server appliance GUI installer to restore a vCenter Server to an ESXi host or a vCenter Server instance. The restore procedure has two stages. The first stage deploys a new vCenter Server appliance. The second stage populates the newly deployed vCenter Server appliance with the data stored in the file-based backup.

Figure 3-1. vCenter Server Restore Workflow



Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See .

- If the vCenter Server instance is part of a vCenter High Availability cluster, you must power off the active, passive, and witness nodes of the cluster before restoring the vCenter Server.

Procedure

1 Stage 1 - Deploy a New Appliance

   In stage 1 of the restore process, you deploy the OVA file, which is included in the vCenter Server GUI installer.

2 Stage 2 - Transfer Data to the Newly Deployed Appliance

   After the OVA deployment finishes, you are redirected to stage 2 of the restore process in which the data from the backup location is copied to the newly deployed vCenter Server appliance.

Stage 1 - Deploy a New Appliance

In stage 1 of the restore process, you deploy the OVA file, which is included in the vCenter Server GUI installer.

As an alternative to performing the first stage of the restore with the GUI installer, you can deploy the OVA file of the new vCenter Server appliance by using the vSphere Client. After the OVA deployment, you must log in to the vCenter Server Management Interface of the newly deployed appliance to proceed with the second stage of the restore process. See "Deploy an OVF or OVA Template" in *vSphere Virtual Machine Administration* vSphere Virtual Machine Administration for information about deploying an OVA file using the vSphere Client.

Prerequisites

- Download and mount the vCenter Server installer. See Download and Mount the vCenter Server Installer.

  Note If you are restoring a backup from a product that has a vCenter Server product patch applied, you must download the ISO of that particular patch. See https://my.vmware.com/group/vmware/patch to search for the vCenter Server product patch. If you cannot locate the patch, search the VMware patch portal at http://www.vmware.com/patchmgr/download.portal.

- If you plan to restore the vCenter Server on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode or part of a fully-automated DRS cluster.
- If you plan to restore the vCenter Server on a DRS cluster of a vCenter Server inventory, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to assign a static IP address to the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you are attempting to restore a vCenter Server instance that is still running, power off the backed up vCenter Server before you start the restore operation.

Procedure

1 In the vCenter Server 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 **Restore**.
3 Review the Introduction page to understand the restore process and click **Next**.
4 Read and accept the license agreement, and click **Next**.
5 On the Enter backup details page, enter the details of the backup file that you want to restore, and click **Next**.

Option	Description
Backup location	Enter the server address and backup folder where the backup files are stored. Specify the protocol to use to retrieve the backup from your backup server. You can select FTP, FTPS, HTTP, HTTPS, or SFTP. You can also enter the IP address or hostname of the backup server and browse for the location of the backup folder. **Note** If you enter the incorrect version of a backup, a warning provides the information required to download the correct version.
User name	Enter the user name of a user with **read** privileges on the backup server.
Password	Enter the password of the user with **read** privileges on the backup server.

6 Review the backup information, and click **Next**.

7 Connect to the ESXi host or vCenter Server on which you want to deploy the vCenter Server appliance to use for the restore operation.

Option	Steps
You can connect to an ESXi host on which to deploy the appliance to use for the restore operation.	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 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target ESXi host, and click **Yes** to accept the certificate thumbprint.
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 appliance to use for the restore operation.	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 user with vCenter Single Sign-On administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4 Click **Next**. 5 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target vCenter Server instance, and click **Yes** to accept the certificate thumbprint. 6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the 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 appliance, and click **Next**.

8 Accept the certificate warning.

9 Enter a name for the vCenter Server appliance, set up the password for the root user, and click **Next**.

10 Select the deployment size for the new vCenter Server appliance depending on the size of your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 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 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 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 restoring.

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 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

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

13 On the Configure network settings page review the settings populated from the backup file of the vCenter Server.

14 (Optional) Edit the network configuration to match the current network environment where the vCenter Server is restored.

15 On the Ready to complete stage 1 page, review the deployment settings for the restored 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 restore process to transfer the data to the newly deployed appliance.

Note If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface to transfer the data.

Results

The newly deployed vCenter Server appliance is running on the target server but the data is not copied from the backup location.

Stage 2 - Transfer Data to the Newly Deployed Appliance

After the OVA deployment finishes, you are redirected to stage 2 of the restore process in which the data from the backup location is copied to the newly deployed vCenter Server appliance.

Procedure

1. Review the introduction to stage 2 of the restore process and click **Next**.
2. Review the backup details and click **Next**.
3. If you are restoring a node with enhanced linked mode support for vCenter Server appliance, you are asked to provide the Single Sign-On credentials. Enter the Single Sign-On user name and password, then click **Validate and Recover**.
4. On the Ready to complete page, review the details, click **Finish**, and click **OK** to complete stage 2 of the restore process.

   The restore process restarts the vCenter Server Management Service. You cannot access the vCenter Server Management API during the restart.

   Important If a restore operation of a vCenter Server appliance VM results with a failure, you must power off and delete the partially restored VM. After that you can try to restore the VM again.
5. (Optional) After the restore process finishes, click the **https://*vcenter_server_appliance_fqdn*/ui** to go to the vSphere Client and log in to the vCenter Server instance , or click the **https://*vcenter_server_appliance_fqdn*:443** to go to the vCenter Server Getting Started page.
6. Click **Close** to exit the wizard.

   You are redirected to the vCenter Server Getting Started page.
7. If the backed up vCenter node is part of a vCenter High Availability cluster, the last needs to be reconfigured after the restore operation completes successfully.

   For information about how to perform backup and restore operations, see *vSphere Availability*.

What to do next

After successful completion of the restore operation, in the event of a total loss of all storage and servers where all the physical hardware or the data in the hardware is lost, follow the instructions in the VMware knowledge base article at http://kb.vmware.com/kb/76585 in order to recover the system to a pre-restore state at the time of the backup.

Image-Based Backup and Restore of a vCenter Server Environment 4

You can use vSphere APIs with a third-party product to back up and restore a virtual machine that contains vCenter Server.

You can perform a full image backup of a virtual machine that contains vCenter Server. The virtual machine must use a fully qualified domain name (FQDN) with correct DNS resolution, or the hostname must be configured to be an IP address.

This chapter includes the following topics:

Considerations and Limitations for Image-Based Backup and Restore

When you restore a vCenter Server environment, take into account these considerations and limitations.

Note Restoring a vCenter Server instance with DHCP network configuration results in changing its IP address. The changed IP address prevents some vCenter Server services from starting properly. To start all vCenter Server services successfully, after the restore, you must reconfigure the IP address of the restored vCenter Server instance to the IP address that the instance was set to when you performed the backup.

Synchronizing Clocks with NTP Time Synchronization Prior to Backup

Before creating a backup of your vCenter Server deployment, verify that all components on the vSphere network have their clocks synchronized using NTP time synchronization. See Synchronizing Clocks on the vSphere Network.

Configuration

After a restore, the following configurations revert to the state when the backup was taken.

- Virtual machine resource settings

- Resource pool hierarchy and setting
- Cluster-host membership
- DRS configuration and rules

Storage DRS

If the configuration changes, the following might change after a restore.

- Datastore Cluster configuration
- Datastore Cluster membership
- Datastore I/O Resource Management (Storage I/O Control) settings
- Datastore-Datacenter membership
- Host-Datastore membership

Distributed Power Management

If you put a host into standby mode after a backup, the vCenter Server might force the host to exit standby mode when you restore to the backup.

Distributed Virtual Switch

If you use a distributed virtual switch, you are advised to export separately the distributed virtual switch configuration before you restore to a backup. You can import the configuration after the restore. If you omit this consideration, you may lose the changes made to a distributed virtual switch after the backup. For detailed steps, see the VMware Knowledge Base article at http://kb.vmware.com/kb/2034602.

Content Libraries

If you delete libraries or items after a backup, you cannot access or use these libraries or items after the restore. You can only delete such libraries or items. A warning message notifies you that there are missing files or folders in the storage backup.

If you create new items or item files after the backup, the Content Library Service has no record of the new items or files after the restore operation. A warning notifies you that extra folders or files were found on the storage backup.

If you create new libraries after the backup, the Content Library Service has no record of the new libraries after restore. The library content exists on the storage backing, but no warning is displayed. You must manually clean the new libraries.

Virtual Machine Life Cycle Operations

- Restoring vCenter Server from a backup that was taken while there are in-flight relocation operations within the vCenter Server instance.

After you restore vCenter Server, the vCenter Server view of the virtual machines may be out of sync with the ESXi view of the virtual machines. This is also true if you performed the backup while there were in-flight operations on vCenter Server. If virtual machines disappear after you restore vCenter Server, you can refer to the following cases.

a The missing virtual machine is located on the destination ESXi host and is registered with the destination ESXi host, but it is not in the vCenter Server inventory. You must manually add the virtual machine to the vCenter Server inventory.

b The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host and it is not in the vCenter Server inventory. You must manually register the virtual machine to the ESXi and add the virtual machine back to the vCenter Server inventory.

c The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host. Within the vCenter Server instance, the missing virtual machine is marked as orphaned. You must remove the virtual machine from the vCenter Server inventory and add it again.

- Restoring vCenter Server from a backup that has an out of date linked clone virtual machine layout.

  If you create a linked clone virtual machine after the backup and you restore vCenter Server from the old backup, then after the restore, vCenter Server does not know about the new linked clone virtual machine until vCenter Server discovers the new linked clone virtual machine. If you remove all existing virtual machines before the new linked clone virtual machine is discovered, then the removal of existing virtual machines corrupts the new linked clone due to missing disks. To avoid this corruption, you must wait until all linked clone virtual machines get discovered by the vCenter Server before you remove virtual machines.

vSphere High Availability

Restoring vCenter Server from a backup may cause it to roll back to older version for the vSphere HA cluster state (HostList, ClusterConfiguration, VM protection state) while the hosts in the cluster have the latest version for the cluster state. Ensure that the vSphere HA cluster state stays the same during restore and backup operations. Otherwise, the following potential problems are present.

- If hosts are added or removed to/from the vSphere HA cluster after backup and before vCenter Server restore, virtual machines could potentially fail over to hosts not managed by the vCenter Server but are still part of the HA cluster.
- Protection states for new virtual machines are not updated on the vSphere HA agents on the hosts which are part of the vSphere HA cluster. As a result, virtual machines are not protected/unprotected.
- New cluster configuration state is not updated on the vSphere HA agents on the hosts which are part of the vSphere HA cluster.

vCenter High Availability

Restoring vCenter Server requires vCenter HA to be reconfigured.

Storage Policy Based Management

Restoring vCenter Server from a backup can lead to the following inconsistencies related to storage policies, storage providers, and virtual machines.

- Registered storage providers after backup are lost.
- Unregistered storage providers after backup reappear and might show different provider status.
- Changes, such as create, delete, or update, performed on storage policies after backup are lost.
- Changes, such as create, delete, or update, performed on storage policy components after backup are lost.
- Default policy configuration changes for datastores performed after backup are lost.
- Changes in the storage policy association of the virtual machine and its disks, and in their policy compliance might occur.

Virtual Storage Area Network

Restoring vCenter Server from a backup may cause inconsistencies in the vSAN. For information how to check vSAN health, see *Administering VMware vSAN*.

Patching

Restoring vCenter Server from a backup might result in missing security patches. You must apply them again after the restore is complete. For information on patching the vCenter Server appliance, see *vSphere Upgrade*.

Restore a vCenter Server Image-based Environment

You can use a third-party product that uses vSphere APIs to restore a virtual machine that contains vCenter Server.

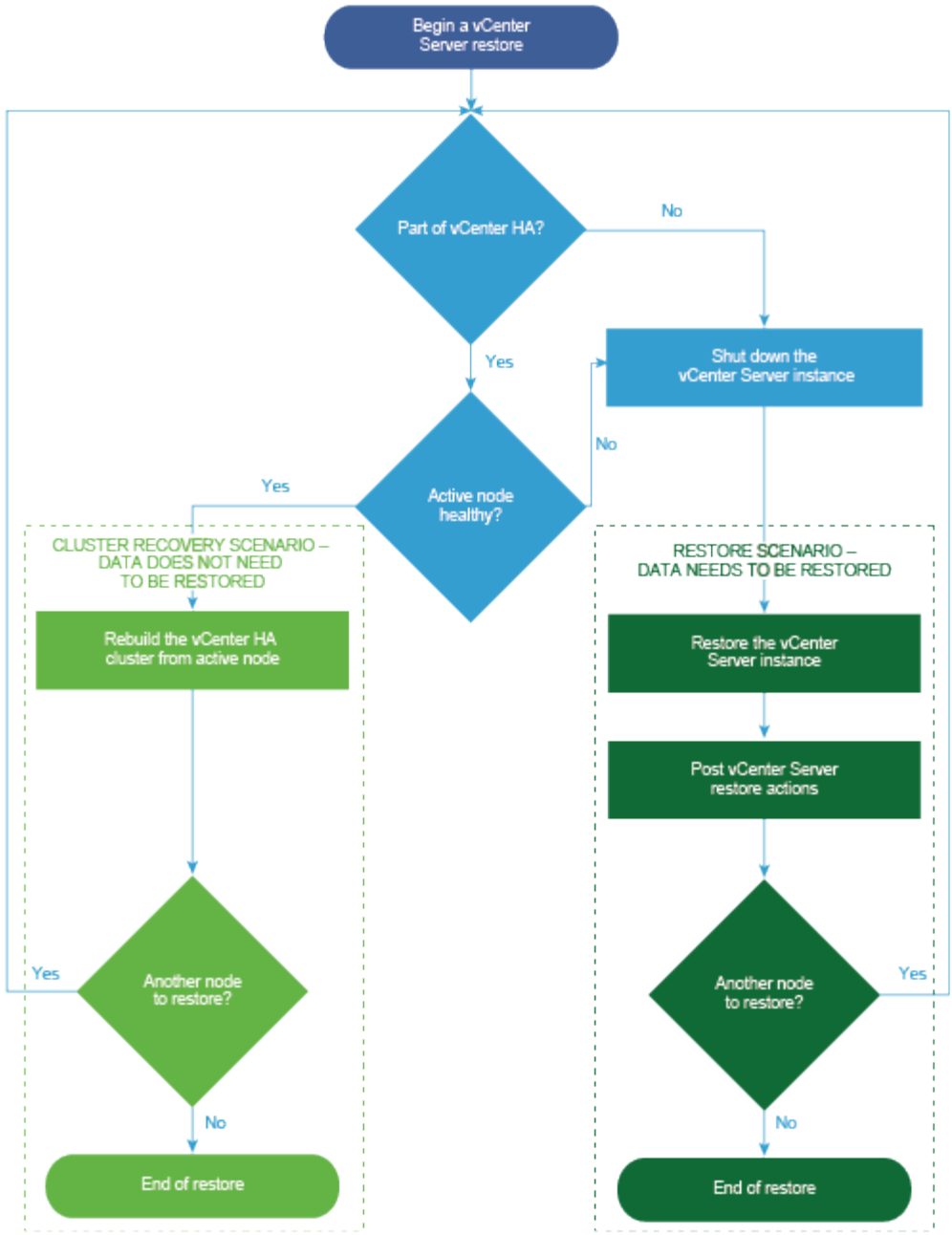
You can perform an image-based restore of a virtual machine that contains vCenter Server. The virtual machine must use a fully qualified domain name (FQDN) with correct DNS resolution, or the host name of the machine must be configured to be an IP address.

You can restore a virtual machine to the original location by either overwriting the backed up virtual machine or by creating a new virtual machine that contains the restored vCenter Server on the same ESXi host. You can also restore the virtual machine on a new ESXi host.

You can restore a virtual machine that contains vCenter Server directly on the ESXi host that is running the third-party appliance when the vCenter Server service becomes unavailable or when you cannot access the third-party user interface by using the vSphere Client.

Important Restoring virtual machines that have snapshots or that are configured with Fault Tolerance is unsupported.

Figure 4-1. vCenter Server Restore Workflow



Restore a vCenter Server Instance

You can use a third-party product to restore a vCenter Server environment.

Important You can back up and restore only virtual machines that contain vCenter Server instances. You cannot back up and restore physical machines that are running vCenter Server by using a third-party product.

Procedure

1. Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.
2. Use the `service-control --status --all` command to verify that the services have started.

   Wait for all the vCenter Server services to start, which can take several minutes.
3. Log into the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
4. Run the reconciliation operation and provide the Single Sign-On credentials.

What to do next

Power on the restored virtual machine that contains the restored vCenter Server instance.

Restore a vCenter Server Environment with a Single Platform Services Controller

Your environment might consist of many vCenter Server instances that are registered with a single Platform Services Controller. You can use a third-party solution to restore a virtual machine that contains a Platform Services Controller. You can also use the third-party solution to restore either virtual machines that contain vCenter Server instances or vCenter Server Appliance instances that are registered with a single external Platform Services Controller.

If the vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instance.

Procedure

1. Restore the Platform Services Controller virtual machine onto the ESXi host using a third-party solution.

   Wait for all the Platform Services Controller services to start, which can take several minutes.
2. After the restore succeeds, in the node associated with that Platform Services Controller, run the following commands.

   ```
   service-control --stop --all
   service-control --start --all
   ```
3. Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.

   The services are masked and are not running.

4 Use the `systemctl status applmgmt` command to verify that the `systemd` instance of the `applmgmt` service has started.

   Wait for all the vCenter Server services to start, which can take several minutes.

5 Log into the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.

6 Run the reconciliation operation and provide the Single Sign-On credentials.

   Do not unmask any services, and do not run the reconciliation script directly.

What to do next

Power on the restored virtual machine that contains the restored vCenter Server instance.

Restore a vCenter Server Environment with Multiple External Platform Services Controller Instances

You can use a third-party solution to restore an environment in which the vCenter Server instances are registered with different Platform Services Controller instances, and in which the infrastructure data is replicated between the Platform Services Controller instances.

Important You can back up and restore only virtual machines that contain vCenter Server instances. You cannot back up and restore physical machines that are running vCenter Server by using a third-party product.

For a vCenter Server with an external Platform Services Controller, you can only restore the last node in the cluster. If it is not the last node in the cluster, deploy a new Platform Services Controller node and join the cluster.

For the last Platform Services Controller in the cluster, use the third-party solution to restore the vCenter Server virtual machine onto the ESXi host. You do not need to perform reconciliation.

Procedure

1 Restore the Platform Services Controller virtual machine onto the ESXi host using a third-party solution.

   Wait for all the Platform Services Controller services to start, which can take several minutes.

2 After the restore succeeds, in the node associated with that Platform Services Controller, run the following commands.

```
service-control --stop --all
service-control --start --all
```

3 Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.

   The services are masked and are not running.

4 Use the `systemctl status applmgmt` command to verify that the `systemd` instance of the `applmgmt` service has started.

   Wait for all the vCenter Server services to start, which can take several minutes.

5 Log into the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.

6 Run the reconciliation operation and provide the Single Sign-On credentials.

   Do not unmask any services, and do not run the reconciliation script directly.

What to do next

Power on the restored virtual machine that contains the restored vCenter Server and Platform Services Controller instances.

Restore a vCenter Enhanced Linked Mode Environment

You can restore a vCenter Enhanced Linked Mode environment using a third-party solution.

Important You can back up and restore only virtual machines that contain vCenter Server instances. You cannot back up and restore physical machines that are running vCenter Server by using a third-party product.

Procedure

1 Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.

   The services are masked and are not yet running.

2 Use the `systemctl status applmgmt` command to verify that the `systemd` instance of the `applmgmt` service has started.

   Wait for all the vCenter Server services to start, which can take several minutes.

3 Log into the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.

4 Run the reconciliation operation and provide the Single Sign-On credentials.

   Do not unmask any services, and do not run the reconciliation script directly.

5 If you are restoring the last embedded node in a vCenter Enhanced Linked Mode group, run the reconciliation operation with the `ignore_warnings` flag selected.

What to do next

Power on the restored virtual machine that contains the restored vCenter Server instance.

After You Deploy the vCenter Server Appliance

5

After you deploy the vCenter Server appliance, consider these post installation options before adding inventory for the vCenter Server to manage.

For information about configuring the vSphere Authentication Proxy service, see *vSphere Security*.

For information about upgrading vCenter Server, see *vCenter Server Upgrade*.

This chapter includes the following topics:

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 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)**.

   You can instead open a Web browser and enter the URL for the vSphere Client: **`https://`***`vcenter_server_ip_address_or_fqdn`***`/ui`**.
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**.

Results

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.

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.

Note When you enable Active Directory Federation Services, Enhanced Authentication Plug-in applies only to configurations where vCenter Server is the identity provider (Active Directory over LDAP, Integrated Windows Authentication, and OpenLDAP configurations).

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

Procedure

1. Open a Web browser and type the URL for the vSphere Client.
2. At the bottom of the vSphere 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.

Repoint vCenter Server to Another vCenter Server in a Different Domain

You can move a vCenter Server from one vSphere domain to another vSphere domain. Services such as tagging and licensing are retained and migrated to the new domain.

The following use cases are supported:

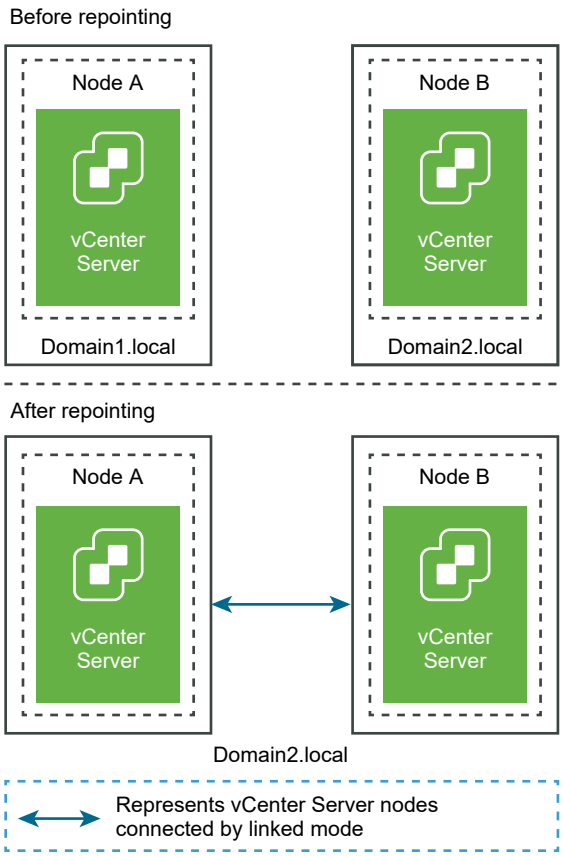
- You can migrate a vCenter Server from an existing domain to an another existing domain with or without replication. The migrated vCenter Server moves from its current Single Sign-On domain and joins the other existing domain as another vCenter Server connected via enhanced linked mode.
  - See Repoint a Single vCenter Server Node from One Domain to an Existing Domain for instructions on repointing a single embedded node from one domain to an existing domain without a replication partner.
  - See Repoint a vCenter Server Node from One Domain to an Existing Domain with a Replication Partner for instructions on repointing an embedded node from one domain to an existing domain using replication.
- You can migrate a vCenter Server from an existing domain to a newly created domain (where the migrated vCenter Server is the first instance). See Repoint a vCenter Server Node to a New Domain for instructions of this type of repointing. In this case, there is no replication partner.

Repoint a Single vCenter Server Node from One Domain to an Existing Domain

You can repoint a single vCenter Server from one Single Sign-On domain to an existing Single Sign-On domain without a replication partner. Each Single Sign-On domain contains a single vCenter Server.

See Figure 5-1. Repointing a Single vCenter Server from One Domain to an Existing Domain for an example of repointing a single vCenter Server from one domain to another existing domain. This is one of many ways to create an Enhanced Linked Mode node. In this case, there is no replication.

Figure 5-1. Repointing a Single vCenter Server from One Domain to an Existing Domain



Prerequisites

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- To ensure no loss of data, take a file-based backup of each node before proceeding with repointing the vCenter Server.

Procedure

1. Make sure that both vCenter Server nodes are powered on before beginning the repointing process.

2 (Optional) Run the pre-check mode command. The pre-check mode fetches the tagging (tags and categories) and authorization (roles and privileges) data from the vCenter Server. Pre-check does not migrate any data, but checks for conflicts between the source and destination vCenter Server. For example, run the pre-check with the following CLI:

```
cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

Note Pre-check is not required if a replication partner does not exist (repointing to a newly created domain).

See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

The pre-check writes the conflicts to the `/storage/domain-data` directory.

3 (Optional) Review the conflicts and apply resolutions for all conflicts, or apply a separate resolution for each conflict.

The conflict resolutions are:

- Copy: Create a duplicate copy of the data in the target domain.
- Skip: Skips copying the data in the target domain.
- Merge: Merges the conflict without creating duplicates.

Note The default resolution mode for Tags and Authorization conflicts is Copy, unless overridden in the conflict files generated during pre-check.

4 Run the `execute` command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, repointing without a replication partner, run the `execute` command with the following:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

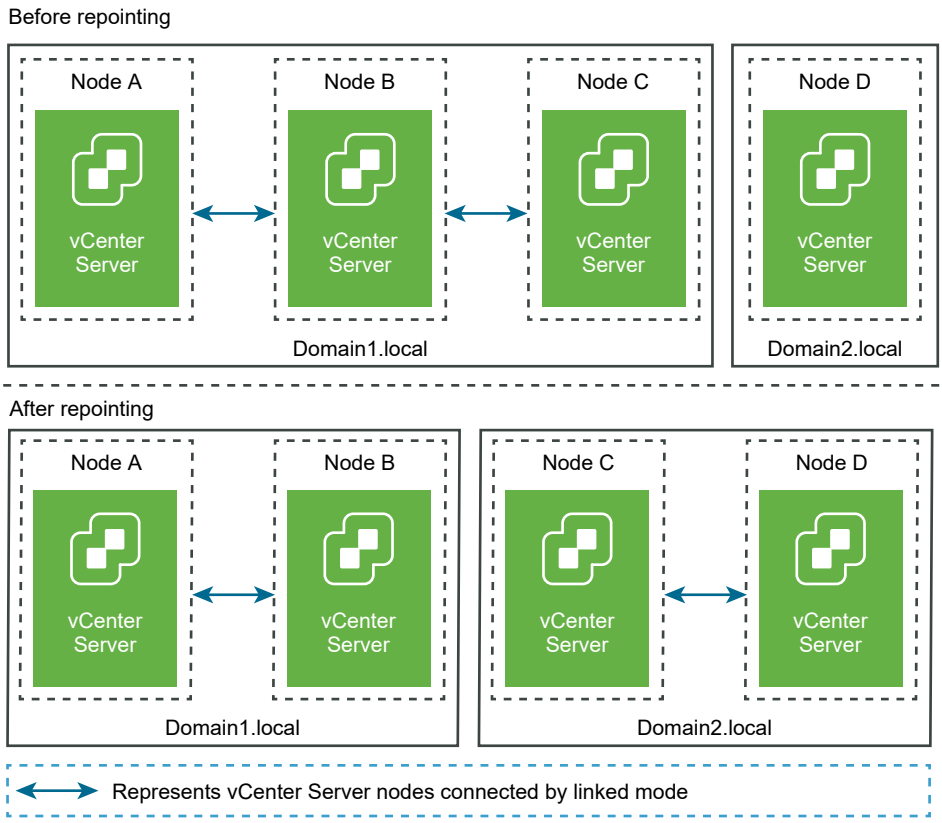
See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

Repoint a vCenter Server Node from One Domain to an Existing Domain with a Replication Partner

You can repoint a vCenter Server from one Single Sign-On domain to an existing domain using a replication partner.

See Figure 5-2. Repointing a vCenter Server from One Domain to an Existing Domain for an example of repointing to an existing domain. In this case, there is repliacation.

Figure 5-2. Repointing a vCenter Server from One Domain to an Existing Domain



Prerequisites

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- To ensure no loss of data, take a file-based backup of each node before proceedeing with repointing the vCenter Server.

Procedure

1. Shut down the node (for example, Node C) that is being repointed (moved to a different domain).
2. Decommission the vCenter Server node that is being repointed. For example, to decommission Node C, log into Node B (on the original domain) and run the following command:

   ```
   cmsso-util unregister --node-pnid Node_C_FQDN --username Node_B_sso_administrator@sso_domain.com
   --passwd Node_B_sso_adminuser_password
   ```

   After unregistering Node C, services are restarted. References to Node C are deleted from Node B and any other nodes that were linked with Node C on the original domain.
3. Power on Node C to begin the repointing process.

4 (Optional) Run the pre-check mode command. The pre-check mode fetches the tagging (tags and categories) and authorization (roles and privileges) data from the vCenter Server. Pre-check does not migrate any data, but checks the conflicts between the source and destination vCenter Server. For example, run the pre-check with the following CLI:

```
cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

Note Pre-check is not required if a replication partner does not exist (repointing to a newly created domain).

See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

The pre-check writes the conflicts to the `/storage/domain-data` directory.

5 (Optional) Check conflicts and apply resolutions for all conflicts or apply a separate resolution for each conflict.

The conflict resolutions are:

- Copy: Create a duplicate copy of the data in the target domain.
- Skip: Skips copying the data in the target domain.
- Merge: Merges the conflict without creating duplicates.

Note The default resolution mode for Tags and Authorization conflicts is Copy, unless overridden in the conflict files generated during pre-check.

6 Run the execute command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, run the execute command with the following:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN _of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

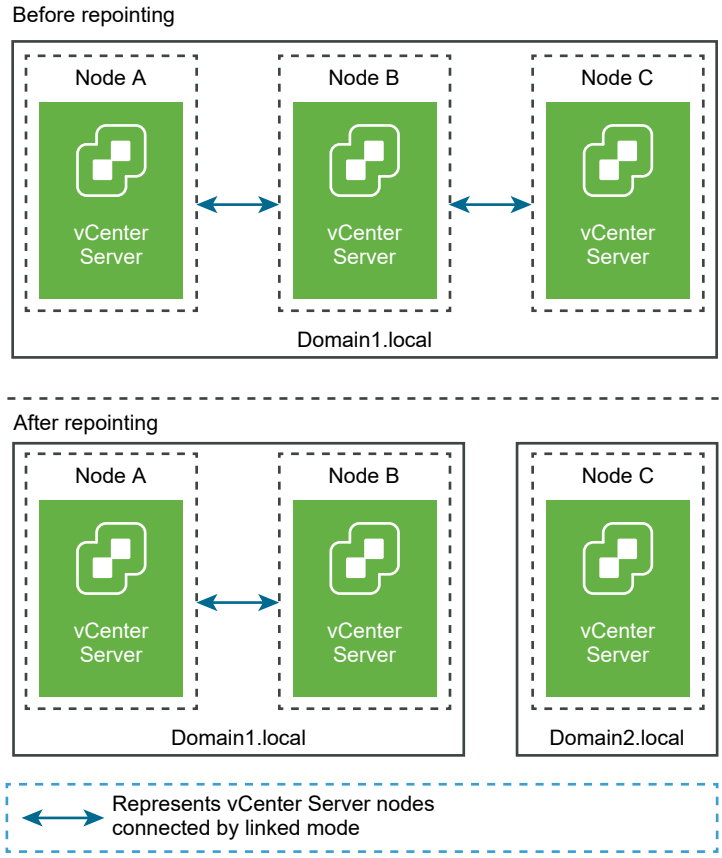
See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

Repoint a vCenter Server Node to a New Domain

You can repoint a vCenter Server from an existing domain to a newly created domain.

See Figure 5-3. Repointing a vCenter Server from One Domain to a New Domain for an example of repointing to a new domain. In this case, there is no replication partner.

Figure 5-3. Repointing a vCenter Server from One Domain to a New Domain



Prerequisites

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- To ensure no loss of data, take a file-based backup of each node before proceeding with repointing the vCenter Server.

Procedure

1. Shut down the node (for example, Node C) that is being repointed (moved to a different domain).
2. Decommission the vCenter Server node that is being repointed. For example, to decommission Node C, log into Node B (on the original domain) and run the following command:

   ```
   cmsso-util unregister --node-pnid Node_C_FQDN --username Node_B_sso_administrator@sso_domain.com
   --passwd Node_B_sso_adminuser_password
   ```

   After unregistering Node C, services are restarted. References to Node C are deleted from Node B and any other nodes that were linked with Node C on the original domain.
3. Power on Node C to begin the repointing process.

4 Run the execute command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, repointing with no replication partner (repointing to a new domain), run the execute command with the following:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator  --dest-domain-name
destination_PSC_domain
```

See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

Syntax of the Domain Repoint Command

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

The `cmsso-util domain-repoint` CLI repoints vCenter Server from one domain to another.

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

Use the following command to repoint a vCenter Server to another vCenter Server node:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN
_of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-
name destination_PSC_domain
```

Argument	Description
`-m`, `--mode`	*mode* can be `pre-check` or `execute`. The `pre-check` argument runs the command in pre-check mode. The `execute` argument runs the command in execute mode.
`-spa`, `--src-psc-admin`	SSO administrator user name for the source vCenter Server. Do not append the *@domain*.
`-dpf`, `--dest-psc-fqdn`	The FQDN of the vCenter Server to repoint.
`-dpa`, `--dest-psc-admin`	SSO administrator user name for the destination vCenter Server. Do not append *@domain*.
`-ddn`, `--dest-domain-name`	SSO domain name of the destination vCenter Server.
`-dpr`, `--dest-psc-rhttps`	(Optional) HTTPS port for the destination vCenter Server. If not set, the default `443` is used.
`-dvf`, `--dest-vc-fqdn`	The FQDN of the vCenter Server pointing to a destination vCenter Server. The vCenter Server is used to check for component data conflicts in the pre-check mode. If not provided, conflict checks are skipped and the default resolution (COPY) is applied for any conflicts found during the import process. **Note** This argument is optional only if the destination domain does not have a vCenter Server. If a vCenter Server exists in the destination domain, this argument is mandatory.

Argument	Description
-sea, --src-emb-admin	Administrator for the vCenter Server with embedded vCenter Server. Do not append @domain to the administrator id.
-rpf, --replication-partner-fqdn	(Optional) The FQDN of the replication partner node to which the vCenter Server is replicated.
-rpr, --replication-partner-rhttps	(Optional) The HTTPS port for the replication node. If not set, the default is 443.
-rpa, --replication-partner-admin	(Optional) SSO administrator user name of the replication partner vCenter Server.
-dvr, --dest-vc-rhttps	(Optional) The HTTPS port for the vCenter Server pointing to the destination vCenter Server. If not set, the default 443 is used.
--ignore-snapshot	(Optional) Ignore snapshot warnings.
--no-check-certs	(Optional) Ignore certification validations.
--debug	(Optional) Retrieves command execution detail.
-h, --help	(Optional) Displays the help message for the cmsso-util domain repoint command.

Understanding Tagging and Authorization Conflicts

When you run the domain repoint command in pre-check mode, data from the vCenter Server is exported, examined, and conflicts are written to a file.

The following data is exported to the /storage/domain-data/ or ProgramData/VMWare/vCenterServerdata/domain-data folder:

- All_Privileges.json
- All_Roles.json
- All_TagCategories.json
- All_Tags.json

These files contain the all the data (Authorization and Tagging) from the vCenter Server on which this command was run.

If a secondary vCenter Server is provided using the -dvf or --dest-vc-fqdn option, any conflicts are also exported to the same folder:

- Conflicts_Roles.json
- Conflicts_TagCategories.json
- Conflicts_Tags.json

The following is a sample conflicts file:

```
<---- Sample Conflict file code block --->
     {
  "global" : {
    "resolution" : "MERGE|SKIP|COPY",
    "description" : "Default resolution option used to resolve Role Conflicts is COPY. The
conflicts list describes the differences between Role entities on source and target vCenter Server.
If
the source information represents an empty JSON array, it simply means that all the entity
attributes from source and target are identical. If the source lists few entries, it means
that only these entity attributes are missing from the target. If the target lists few entries,
it means that only these entity attributes are missing from the source. Though a global resolution
can be set, it can also be overridden at each conflict level by providing individual resolution
mode."
  },
  "conflicts-count" : 1,
  "conflicts-list" : {
    "NoCryptoAdmin" : {
      "source" : {
        "privileges" : "[]"
      },
      "target" : {
        "privileges" : "[Group-1.SamplePriv-1, Group-1.SamplePriv-4, Group-2.SamplePriv-10,
Group-2.SamplePriv-3, Group-2.SamplePriv-7, Group-3.SamplePriv-2, Group-3.SamplePriv-9]"
      },
      "resolution" : ""
    }
}
<----- End of code block --->
```

The parts of the sample conflict files are:

- `description`. Provides the details on how the respective conflicts file is read and understood.
- `source` and `target`. JSON objects that list only the differences between the source and target vCenter Server objects.
- `resolution`. User supplies one valid resolution. Valid resolutions are `MERGE`, `COPY`, and `SKIP`.

To specify the resolution for handling conflicts, you can provide a default resolution option all conflicts in the `"global": "resolution" = "MERGE|SKIP|COPY"` section. If you do not provide a valid global resolution type for `resolution` or leave it unedited, the system uses `COPY` as the default resolution option.

You can also provide a valid resolution option for each of the conflicts by editing the `resolution` property at each conflict level which overrides the global resolution option.

The types of conflicts listed in Table 5-1. Conflict Types.

Table 5-1. Conflict Types

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
Role conflict	■ `name`: Name of the category. ■ `privilegeId`: List of privileges for the role.	`RoleName` conflict occurs while importing roles and a role with the same name exists in the target vCenter Server but with different privileges.	Properties that can be conflicting for `RoleName` conflict type can be `Privileges`.	■ `COPY`. A copy of the conflicting role is created in the target vCenter Server, with `--copy` appended to the role name. The new role is created with a new role ID with the same set of privilege IDs. The new role ID is updated in the `VPX_ACCESS` table. The new role ID is applicable for both role name conflict and role ID conflict. **Note** The default resolution option to resolve Role conflicts is `COPY`. ■ `MERGE`.The `MERGE` option is resolved in the following sequence: a If the source vCenter Server has a role with the same name and privilege list as a role in the target vCenter Server, but the role IDs are different, the role ID from the target vCenter Server is used and updated in the `VPX_ACCESS` table. b If the source vCenter Server has a role with the same name as a role in the target vCenter Server, but with a different privilege list, then the privilege lists for both roles are merged. ■ `SKIP`. Do nothing. The specific role is skipped.
Tag Category conflict: A category name must be unique	■ `name`: Name of the category.	Only one type of conflict can be seen while importing Tag Categories, `CategoryName`	Properties that can be conflicting for conflict type `CategoryName` can	■ `COPY`. A copy of the conflicting category is created in the target vCenter Server, with `--copy` appended to the category

Table 5-1. Conflict Types (continued)

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
in a vCenter Server.	■ `cardinality`: Cardinality of Category, either Single or Multiple. ■ `associableEntityType` : List of vCenter Server object that can be associated with a tag from this category. A value of `All` indicates all vCenter Server objects.	conflict. This conflict indicates that a category with the same name exists in the target vCenter Server but with different properties (`cardinality` or `associableEntityType`).	be at least one of two types: `Cardinality` or `AssociableTypes`.	name. The new category is created with the same property name as in the source vCenter Server. All the tags that were present under this category is imported under the newly created `CategoryCopy`. **Note** The default resolution option to resolve `CategoryName` conflicts is `COPY`. ■ `MERGE`. Conflicting properties are merged with the category that is already present in the SSO. Properties are merged as follows: a `Description`. The description that is already present is used. b `Cardinality`. Cardinality cannot shrink. If there is a cardinality conflict, the cardinality is set to `multiple`. It cannot be reduced to single. c `AssociableTypes`.If either the `associableEntityType` values are null, it is set to null. Otherwise, `Objects` types are merged. ■ `SKIP`. Do nothing. All tags are imported under the category that exists.
Tags Conflict: A `tag` object always belongs to a `category` Object. A tag Name must be unique only inside a category.	■ `name` ■ `description`	Only one type of conflict can be seen while importing tags: `TagName` conflict. This conflict indicates that a Tag with the same name exists under the same category and in the target vCenter	Properties that can be conflicting for a conflict of type: `TagName` can be `Description`.	■ `COPY`. A copy of the conflicting tag is created in the target vCenter Server, with `--copy` appended to the tag name. Take the `MoRef`(Internal tag ID) of the newly created tag and update the tag association if necessary. **Note**

Table 5-1. Conflict Types (continued)

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
		Server but with different properties.		The default resolution option to resolve `CategoryName` conflicts is `COPY`. ■ `MERGE`.Keep the existing description. Take the `MoRef`(Internal Tag ID) and update one or more Tag Associations if necessary. ■ `SKIP`. Do nothing. Do not create this tag. Clean up any Tag Associations.

vCenter Server Domain Repoint License Considerations

Domain repointing copies license keys to a new domain. Copying the license keys ensures that valid licensing of all assets is maintained after repointing.

vCenter Server tracks license usage on a per domain basis. If a key is used in more than one domain, you must ensure that the aggregate use of the key does not exceed its capacity. To simplify your license management, remove each license copied to a second domain and assign a new license to assets.

Consider the following two cases:

- License keys that are no longer in use (that is, assigned to assets) in the original domain post repointing.
- License keys that are in use (that is, assigned to assets) in multiple domains.

License Keys Not in Use in a Domain

If after completing repointing, a license key appears in more than one domain, but is not in use in some of those domains, you can remove the license key from any domain in which it is not in use. See "Remove Licenses" in *vCenter Server and Host Management* for instructions on how to remove the licenses in vCenter Server.

License Keys in Use in Multiple Domains

If after completing repointing, a license key is in use (that is, assigned to assets) in more than one domain, to remove the license key from all but one domain, first a different license key must be assigned to each asset in domains from which the license key will be removed. Two common approaches:

- If you have other license keys available with sufficient unused capacity, you might use these other keys in place of a license key to be removed. See "Assign a License to Multiple Assets" in *vCenter Server and Host Management* to assign licenses in vCenter Server.

- You might divide the license keys used in more than one domain into separate license keys, one for each domain. To divide the license keys, see the VMware knowledge base article at http://kb.vmware.com/kb/2006972. To determine the capacity to be included in each of the license keys into which the original is divided, see "Viewing Licensing Information" in *vCenter Server and Host Management* to view the usage of the license key in vCenter Server for each of the domains.

  Each of the resulting license keys can then be added to a different domain and assigned in vCenter Server to assets previously licensed with the original license key. See "Create New Licenses" in *vCenter Server and Host Management* to create licenses and "Assign a License to Multiple Assets" in *vCenter Server and Host Management* to assign a license to multiple assets.

  After different licenses are assigned to all assets, the original license key, which is no longer valid, can be removed from all the domains using vCenter Server. See "Remove Licenses" *vCenter Server and Host Management*.

Troubleshooting vCenter Server Installation or Deployment

6

The vCenter Server deployment troubleshooting topics provide solutions to problems that you might encounter during the vCenter Server appliance deployment process.

This chapter includes the following topics:

- Collecting Logs for Troubleshooting a vCenter Server Installation or Upgrade

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 also collect deployment log files for vCenter Server.

- Retrieve Installation Logs Manually

  You can retrieve the installation log files manually for examination.

- Collect Deployment Log Files for the vCenter Server Appliance

  If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

- Export a vCenter Server Support Bundle for Troubleshooting

  You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

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 Deployment Log Files for the vCenter Server Appliance

If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

The full path to the log files is displayed in the vCenter Server appliance deployment wizard.

In case of firstboot failure, you can download the support bundle on a Windows host machine and examine the log files to determine which firstboot script failed. See Export a vCenter Server Support Bundle for Troubleshooting.

Procedure

1 On the Windows machine that you use for deploying the vCenter Server appliance, navigate to the log files folder.

If you are logged in as an administrator, by default this is the `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller` folder.

2 Open the installation log files in a text editor for examination.

Export a vCenter Server Support Bundle for Troubleshooting

You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

You can also collect the support bundle from the vCenter Server appliance Bash shell by running the `vc-support.sh` script.

The support bundle is exported in `.tgz` format.

Procedure

1 Log in to the Windows host machine on which you want to download the bundle.

2 Open a Web browser and enter the URL to the support bundle displayed in the DCUI.

https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3 Enter the user name and password of the root user.

4 Click **Enter**.

The support bundle is downloaded as `.tgz` file on your Windows machine.

5 (Optional) To determine which firstboot script failed, examine the `firstbootStatus.json` file.

If you ran the `vc-support.sh` script in the vCenter Server appliance Bash shell, to examine the `firstbootStatus.json` file, run

```
cat /var/log/firstboot/firstbootStatus.json
```