vCenter Server and Host Management

vmware®

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

https://docs.vmware.com/

Contents

14 Automating Management Tasks by Using vRealize Orchestrator 163

About VMware vCenter Server and Host Management

vCenter Server and Host Management describes how to use the VMware® vSphere Client components, configure and manage hosts, migrate virtual machines, and manage licenses in your vCenter Server environment.

vCenter Server and Host Management also provides brief introductions to the various tasks you can perform within the system, and it cross-references to the documentation that describes the tasks in detail.

vCenter Server and Host Management covers ESXi and vCenter Server.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

vCenter Server and Host Management is intended for system administrators who are experienced Windows or Linux system administrators and who are familiar with virtual machine technology and data center operations.

Updated Information

This *vCenter Server and Host Management* guide is updated with each release of the product or when necessary.

This table provides the update history of the *vCenter Server and Host Management* guide.

Revision	Description
02 APR 2021	■ VMware has rebranded the My VMware portal as VMware Customer Connect. We updated the *vCenter Server and Host Management* documentation to reflect this name change. ■ Minor changes.
09 MAR 2021	Initial release.

vSphere Concepts and Features

1

VMware vSphere® uses the power of virtualization to transform data centers into simplified cloud computing infrastructures, enabling IT organizations to deliver flexible and reliable IT services.

The two core components of vSphere are VMware ESXi™ and VMware vCenter Server®. ESXi is the hypervisor on which you create and run virtual machines. vCenter Server is a service that acts as a central administrator for ESXi hosts that are connected on a network. With vCenter Server, you can pool and manage the resources of multiple hosts. vCenter Server allows you to monitor and manage your physical and virtual infrastructure.

Additional vSphere components are available as plugins that extend the functionality of the vSphere product.

This chapter includes the following topics:

- Virtualization Basics
- Physical Topology of vSphere Data Center
- vSphere Software Components
- vSphere Cluster Services (vCLS)
- Client Interfaces for vSphere
- vSphere Managed Inventory Objects
- Optional vCenter Server Components
- vCenter Server Plug-Ins

Virtualization Basics

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The hypervisor serves as a platform for running virtual machines and allows for the consolidation of computing resources.

Each virtual machine contains its own virtual, or software-based, hardware, including a virtual CPU, memory, hard disk, and network interface card.

ESXi is the hypervisor in a vSphere environment. The hypervisor is installed on physical or virtual hardware in a virtualized data center, and acts as a platform for virtual machines. The hypervisor provides physical hardware resources dynamically to virtual machines to support the operation of the virtual machines. The hypervisor allows virtual machines to operate with a degree of independence from the underlying physical hardware. For example, a virtual machine can be moved from one physical host to another, or its virtual disks can be moved from one type of storage to another, without affecting the functioning of the virtual machine.

Because virtual machines are decoupled from the underlying physical hardware, virtualization allows you to consolidate physical computing resources such as CPUs, memory, storage, and networking into pools of resources. These resources can be dynamically and flexibly made available to virtual machines. With the vCenter Server management platform, you can increase the availability and security of your virtual infrastructure.

Physical Topology of vSphere Data Center

A typical VMware vSphere data center consists of physical building blocks such as x86 virtualization servers, storage networks and arrays, IP networks, a management server, and desktop clients.

The vSphere data center includes the following components.

ESXi Hosts

Industry standard x86 servers that run ESXi on the bare metal. ESXi software provides resources for and runs the virtual machines. You can group a number of similarly configured x86 servers with connections to the same network and storage subsystems. This grouping creates an aggregate set of resources in the virtual environment, called a cluster.

Storage networks and arrays

VMware vSphere uses Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays to meet different data center storage needs. With storage area networks, you can connect and share storage arrays between groups of servers. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines. For detailed information, see *vSphere Storage*.

IP networks

Each compute server can have multiple physical network adapters to provide high bandwidth and reliable networking to the entire VMware vSphere data center. For detailed information, see *vSphere Networking*.

vCenter Server

vCenter Server provides a single point of control to the data center. It provides essential data center services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire data center. It manages the assignment of virtual machines to the ESXi hosts and

the assignment of resources to the virtual machines within a given computing server. These assignments are based on the policies that the system administrator sets.

Compute servers continue to function even if vCenter Server becomes unreachable (for example, if the network is severed). The ESXi hosts can be managed separately and continue to run the virtual machines assigned to them based on the resource assignment that was last set. After connection to vCenter Server is restored, it can manage the data center as a whole again.

Management clients

VMware vSphere provides several interfaces for data center management and virtual machine access. These interfaces include vSphere Client for access through a web browser or vSphere Command-Line Interface (vSphere CLI).

vSphere Software Components

VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components that fulfill several different functions in the vSphere environment.

vSphere includes the following software components:

ESXi

The hypervisor runs virtual machines. Each virtual machine has a set of configuration and disk files that together perform all the functions of a physical machine.

Through ESXi, you run the virtual machines, install operating systems, run applications, and configure the virtual machines. Configuration includes identifying the virtual machine's resources, such as storage devices.

The server provides bootstrapping, management, and other services that manage your virtual machines.

vCenter Server

A service that acts as a central administrator for VMware ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the ESXi hosts.

vCenter Server is installed to run automatically on a preconfigured virtual machine. The vCenter Server service runs continuously in the background. It performs its monitoring and managing activities even when no vSphere Clients are connected and when no one is logged on to the computer where it resides. It must have network access to all the hosts it manages.

vCenter Server is deployed as a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy vCenter Server on ESXi hosts 6.5 or later.

All prerequisite services for running vCenter Server and the vCenter Server components are bundled in the vCenter Server installation. All vCenter Server services run as child processes of the VMware Service Library Lifecycle Manager service. See the *vCenter Server Installation and Setup* documentation for details about setting up this configuration.

vCenter Single Sign-On

A service that is part of the vCenter Server management infrastructure. The vCenter Single Sign-On authentication service makes the VMware cloud infrastructure platform more secure by allowing the various vSphere software components to communicate with each other. The vCenter Single Sign-On authentication service uses a secure token exchange mechanism instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

When you install vCenter Single Sign-On, the following components are deployed.

STS (Security Token Service)

STS certificates enable a user who has logged on through vCenter Single Sign-On to authenticate to any vCenter service that vCenter Single Sign-On supports. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in each of the vCenter Single Sign-On identity sources.

Administration server

The administration server allows users with vCenter Single Sign-On administrator privileges to configure the vCenter Single Sign-On service and manage users and groups from the vSphere Client. Initially, only the user administrator@vsphere.local has these privileges.

vCenter Lookup Service

vCenter Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely. Unless you are using Simple Install, you are prompted for the Lookup Service URL when you install other vSphere components. For example, the Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server system are registered with the vCenter Lookup Service so other vSphere components, like the vSphere Client, can find them.

VMware Directory Service

Directory service associated with the vsphere.local domain. This service is a multi-tenanted, peer-replicating directory service that makes an LDAP directory available on port 389. In multisite mode, an update of VMware Directory Service content in one VMware Directory Service instance results in the automatic update of the VMware Directory Service instances associated with all other vCenter Single Sign-On nodes.

vCenter Server plug-ins

Applications that provide additional features and functionality to vCenter Server. Typically, plug-ins consist of a server component and a client component. After the plug-in server is installed, it is registered with vCenter Server and the plug-in client is available to the vSphere Client for download. After a plug-in is installed on the vSphere Client, it might alter the interface by adding views, tabs, toolbar buttons, or menu items related to the added functionality.

Plug-ins leverage core vCenter Server capabilities, such as authentication and permission management, but can have their own types of events, tasks, metadata, and privileges.

Some vCenter Server features are implemented as plug-ins, and can be managed using the vSphere Client Plug-in Manager. These features include vCenter Storage Monitoring, vCenter Hardware Status, and vCenter Service Status.

vCenter Server database

Persistent storage for maintaining the status of each virtual machine, host, and user managed in the vCenter Server environment. The vCenter Server database can be remote or local to the vCenter Server system.

The database is installed and configured during vCenter Server installation.

If you are accessing your ESXi host directly through the VMware Host Client, and not through a vCenter Server system and associated vSphere Client, you do not use a vCenter Server database.

tcServer

Many vCenter Server functions are implemented as web services that require the tcServer. The tcServer is installed on the vCenter Server machine as part of the vCenter Server installation.

Features that require the tcServer to be running include: lCIM/Hardware Status tab, Performance charts, WebAccess, Storage Policy-Based services, and vCenter Service status.

vCenter Server agent

On each managed host, the software that collects, communicates, and runs the actions received from vCenter Server. The vCenter Server agent is installed the first time any host is added to the vCenter Server inventory.

Host agent

On each managed host, the software that collects, communicates, and runs the actions received through the vSphere Client. It is installed as part of the ESXi installation.

vSphere Cluster Services (vCLS)

In vSphere 7.0 U2, vSphere Cluster Services (vCLS) is enabled by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain

available to maintain the resources and health of the workloads that run in the clusters. vCenter Server is still required in 7.0 U2 to run DRS and HA.

vCLS is enabled when you upgrade to vSphere 7.0 U2 or when you have a new vSphere 7.0 U2 deployment. vCLS is upgraded as part of vCenter Server upgrade.

vCLS uses agent virtual machines to maintain cluster services health. The vCLS agent virtual machines (vCLS VMs) are created when you add hosts to clusters. Up to three vCLS VMs are required to run in each vSphere cluster, distributed within a cluster. vCLS is also enabled on clusters which contain only one or two hosts. In these clusters the number of vCLS VMs is one and two, respectively.

Table 1-1. Number of vCLS Agent VMs in Clusters

Number of Hosts in a Cluster	Number of vCLS Agent VMs
1	1
2	2
3 or more	3

vCLS VMs run in every cluster even if cluster services like vSphere DRS or vSphere HA are not enabled on the cluster. The lifecycle operations of vCLS VMs are managed by vCenter services like ESX Agent Manager and Workload Control Plane. In vSphere 7.0 U2, vCLS VMs do not support NiC cards.

A cluster enabled with vCLS can contain ESXi hosts of different versions if the ESXi versions are compatible with vCenter Server 7.0 U2. vCLS works with both vLCM and VUM managed clusters and runs in all vSphere license SKU clusters.

vSphere DRS

vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. In vSphere 7.0 U2, DRS depends on the availability of vCLS VMs.

Note If you try to enable DRS on a cluster where there are issues with the vCLS VMs, a warning message is displayed on the **Cluster Summary** page.

Note If DRS is on but there are issues with the vCLS VMs, you must resolve these issues for DRS to operate. A warning message is displayed on the **Cluster Summary** page.

If DRS is non-functional this does not mean that DRS is disabled. Existing DRS settings and resource pools survive across a lost vCLS VMs quorum. vCLS health turns **Unhealthy** only in a DRS enabled cluster when vCLS VMs are not running and the first instance of DRS is skipped because of this. vCLS health will stay **Degraded** on a non-DRS enabled cluster when at least one vCLS VM is not running.

Datastore selection for vCLS VMs

The datastore for vCLS VMs is automatically selected based on ranking all the datastores connected to the hosts inside the cluster. A datastore is more likely to be selected if there are hosts in the cluster with free reserved DRS slots connected to the datastore. The algorithm tries to place vCLS VMs in a shared datastore if possible before selecting a local datastore. A datastore with more free space is preferred and the algorithm tries not to place more than one vCLS VM on the same datastore. You can only change the datastore of vCLS VMs after they are deployed and powered on.

If you want to move the VMDKs for vCLS VMs to a different datastore or attach a different storage policy, you can reconfigure vCLS VMs. A warning message is displayed when you perform this operation.

You can perform a storage vMotion to migrate vCLS VMs to a different datastore. You can tag vCLS VMs or attach custom attributes if you want to group them separately from workload VMs, for instance if you have a specific meta-data strategy for all VMs that run in a datacenter.

In vSphere 7.0 U2, new anti-affinity rules are applied automatically. Every three minutes a check is performed, if multiple vCLS VMs are located on a single host they will be automatically redistributed to different hosts.

Note When a datastore is placed in maintenance mode, if the datastore hosts vCLS VMs, you must manually apply storage vMotion to the vCLS VMs to move them to a new location or put the cluster in retreat mode. A warning message is displayed.

```
The enter maintenance mode task will start but cannot finish because there is 1 virtual machine
residing on the datastore. You can always cancel the task in your Recent Tasks if you decide to
continue.
```

```
The selected datastore might be storing vSphere Cluster Services VMs which cannot be powered off. To
ensure the health of vSphere Cluster Services, these VMs have to be manually vMotioned to a different
datastore within the cluster prior to taking this datastore down for maintenance. Refer to this KB
article: KB 79892.
```

Select the checkbox
Let me migrate storage for all virtual machines and continue entering maintenance mode after migration. to proceed.

Monitoring vSphere Cluster Services

You can monitor the resources consumed by vCLS VMs and their health status.

vCLS VMs are not displayed in the inventory tree in the **Hosts and Clusters** tab. vCLS VMs from all clusters within a data center are placed inside a separate VMs and templates folder named **vCLS**. This folder and the vCLS VMs are visible only in the **VMs and Templates** tab of the vSphere Client. These VMs are identified by a different icon than regular workload VMs. You can view information about the purpose of the vCLS VMs in the **Summary** tab of the vCLS VMs.

You can monitor the resources consumed by vCLS VMs in the **Monitor** tab.

Table 1-2. vCLS VM Resource Allocation

Property	Size
VMDK size	245 MB (thin disk)
Memory	128 MB
CPU	1 vCPU
Hard disk	2 GB
Storage on datastore	480 MB (thin disk)

Note Each vCLS VM has 100MHz and 100MB capacity reserved in the cluster. Depending on the number of vCLS VMs running in the cluster, a max of 400 MHz and 400 MB of capacity can be reserved for these VMs.

You can monitor the health status of vCLS in the **Cluster Services** portlet displayed in the **Summary** tab of the cluster.

Table 1-3. Health status of vCLS

Status	Color Coding	Summary
Healthy	Green	If there is at least one vCLS VM running, the status remains healthy, regardless of the number of hosts in the cluster.
Degraded	Yellow	If there is no vCLS VM running for less than 3 minutes (180 seconds), the status is degraded.
Unhealthy	Red	If there is no vCLS VM running for 3 minutes or more, the status is unhealthy in a DRS enabled cluster.

Maintaining Health of vSphere Cluster Services

vCLS VMs are always powered-on because vSphere DRS depends on the availability of these VMs. These VMs should be treated as system VMs. No operations are blocked on vCLS VMs, however any disruptive operation can result in failure of vSphere DRS. To avoid failure of cluster services, avoid performing any configuration or operations on the vCLS VMs.

Operations that might disrupt the healthy functioning of vCLS VMs:

- Changing the power state of the vCLS VMs
- Resource reconfiguration of the vCLS VMs such as changing CPU, Memory, Disk size, Disk placement
- VM encryption
- Triggering vMotion of the vCLS VMs

- Changing the BIOS

- Removing the vCLS VMs from the inventory

- Deleting the vCLS VMs from disk

- Enabling FT of vCLS VMs

- Cloning vCLS VMs

- Configuring PMem

- Moving vCLS VM to a different folder

- Renaming the vCLS VMs

- Renaming the vCLS folders

- Enabling DRS rules and overrides on vCLS VMs

- Enabling HA admission control policy on vCLS VMs

- Enabling HA overrides on vCLS VMs

- Moving vCLS VMs to a resource pool

- Recovering vCLS VMs from a snapshot

When you perform any disruptive operation on the vCLS VMs, a warning dialog box appears.

Troubleshooting:

The health of vCLS VMs, including power state, is managed by EAM and WCP services. In case of power on failure of vCLS VMs, or if the first instance of DRS for a cluster is skipped due to lack of quorum of vCLS VMs, a banner appears in the cluster summary page along with a link to a Knowledge Base article to help troubleshoot the error state.

Because vCLS VMs are treated as system VMs, you do not need to backup or snapshot these VMs. The health state of these VMs is managed by vCenter services.

Client Interfaces for vSphere

You can access vSphere components through the vSphere Client, the VMware Host Client, and the vSphere Command-Line Interface.

vSphere Client

The vSphere Client, introduced in vSphere 6.5, is an HTML5-based client and is included with vCenter Server. As of vSphere 7.0, the vSphere Web Client has been deprecated. The vSphere Client is the primary interface for connecting to and managing vCenter Server instances.

VMware Host Client

The VMware Host Client is a Web-based application that you can use to manage individual ESXi hosts that are not connected to a vCenter Server system.

For more information about the VMware Host Client, see *vSphere Single Host Management - VMware Host Client*.

vSphere Command-Line Interfaces

vSphere supports multiple command-line interfaces for configuring virtual machines, ESXi hosts, and vCenter Server.

vSphere Managed Inventory Objects

In vSphere, the inventory is a collection of virtual and physical objects on which you can place permissions, monitor tasks and events, and set alarms. You can group most inventory objects by using folders to more easily manage them.

All inventory objects, with the exception of hosts, can be renamed to represent their purposes. For example, they can be named after company departments or locations or functions.

Note Managed object names cannot exceed 214 bytes (UTF-8 encoded).

vCenter Server monitors and manages the following inventory objects:

Data Centers

Unlike folders, which are used to organize specific object types, a data center is an aggregation of all the different types of objects used to work in virtual infrastructure.

Within each data center, there are four separate hierarchies.

- Virtual machines (and templates)

- Hosts (and clusters)

- Networks

- Datastores

Clusters

A collection of ESXi hosts and associated virtual machines intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit.

Datastores

A virtual representation of physical storage resources in the data center. A datastore is the storage location for virtual machine files. In an on-premises SDDC, these physical storage resources can come from the local SCSI disk of the ESXi host, the Fibre Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. For both on-premises and cloud SDDCs, vSAN datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines.

Folders

Folders allow you to group objects of the same type so you can easily manage them. For example, you can use folders to set permissions across objects, to set alarms across objects, and to organize objects in a meaningful way.

A folder can contain other folders, or a group of objects of the same type: data centers, clusters, datastores, networks, virtual machines, templates, or hosts. For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines.

Hosts

The physical computer on which ESXi is installed. All virtual machines run on hosts or clusters.

Networks

A set of virtual network interface cards (virtual NICs), distributed switches or vSphere Distributed Switches, and port groups or distributed port groups that connect virtual machines to each other or to the physical network outside of the virtual data center. You can monitor networks and set permissions and alarms on port groups and distributed port groups.

Resource pools

Resource pools are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines run in, and draw their resources from, resource pools. You can create multiple resource pools as direct children of a standalone host or cluster and then delegate control over each resource pool to other individuals or organizations.

You can monitor resources and set alarms on them.

Templates

A template is a primary copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed. They can be customized during deployment to ensure that the new virtual machine has a unique name and network settings.

Virtual machines

A virtualized computer environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same managed host machine concurrently.

vApps

vSphere vApp is a format for packaging and managing applications. A vApp can contain multiple virtual machines.

Optional vCenter Server Components

Optional vCenter Server components are packaged and installed with the base product, but might require a separate license.

Optional vCenter Server features include:

vMotion

Enables you to move running virtual machines from one ESXi host to another ESXi host without service interruption. It requires licensing on both the source and target host. vCenter Server centrally coordinates all vMotion activities.

Storage vMotion

Allows you to move the disks and configuration file of a running virtual machine from one datastore to another without service interruption. It requires licensing on the virtual machine's host.

vSphere HA

Enables a cluster with High Availability. If a host fails, all virtual machines that were running on the host are promptly restarted on different hosts in the same cluster.

When you enable the cluster for vSphere HA, you specify the number of hosts you want to be able to recover. If you specify the number of host failures allowed as **1**, vSphere HA maintains enough capacity across the cluster to tolerate the failure of one host. All running virtual machines on that host can be restarted on remaining hosts. By default, you cannot turn on a virtual machine if doing so violates required failover capacity.

vSphere DRS

Helps improve resource allocation and power consumption across all hosts and resource pools. vSphere DRS collects resource use information for all hosts and virtual machines in the cluster and gives recommendations (or migrates virtual machines) in one of two situations:

- Initial placement – When you power on a virtual machine in the cluster for the first time, DRS either places the virtual machine or makes a recommendation.

- Load balancing – DRS attempts to improve resource use across the cluster by performing automatic migrations of virtual machines (vMotion) or by providing a recommendation for virtual machine migrations.

vSphere DRS includes distributed power management (DPM) capabilities. When DPM is enabled, the system compares cluster-level and host-level capacity to the demands of virtual machines that are running in the cluster. Based on the results of the comparison, DPM recommends (or implements) actions that can reduce the power consumption of the cluster.

Storage DRS

Allows you to manage multiple datastores as a single resource, called a datastore cluster. A datastore cluster is an aggregation of multiple datastores into a single logical, load-balanced

pool. You can treat the datastore cluster as a single flexible storage resource for resource management purposes. You can assign a virtual disk to a datastore cluster, and Storage DRS finds an appropriate datastore for it. The load balancer takes care of initial placement and future migrations based on workload measurements. Storage space balancing and I/O balancing minimize the risk of running out of space and the risk of I/O bottlenecks slowing the performance of virtual machines.

vSphere Fault Tolerance

vSphere Fault Tolerance provides continuous availability for virtual machines by creating and maintaining a Secondary VM that is identical to the Primary VM. This Secondary VM is continuously available to replace the Primary VM in a failover situation.

vCenter Server Plug-Ins

vCenter Server plug-ins extend the capabilities of vCenter Server by providing additional features and functions.

Some plug-ins are installed as part of the base vCenter Server product.

vCenter Storage Monitoring

Allows you to review information on storage use and to map relationships visually between all storage entities available in vCenter Server.

vCenter Hardware Status

Uses CIM monitoring to display the hardware status of hosts that vCenter Server manages.

vCenter Service Status

Displays the status of vCenter services.

Some plug-ins are packaged separately from the base product and require separate installation. You can update plug-ins and the base product independently of each other. VMware modules include:

vSphere Lifecycle Manager

Enables administrators to apply updates and patches across ESXi hosts and all managed virtual machines. Administrators can create user-defined security baselines that represent a set of security standards. Security administrators can compare hosts and virtual machines against these baselines to identify and remediate systems that are not in compliance.

vRealize Orchestrator

A workflow engine that enables you to create and run automated workflows in your vSphere environment. vRealize Orchestrator coordinates workflow tasks across multiple VMware products and third-party management and administration solutions through its open plug-in architecture. vRealize Orchestrator provides a library of workflows that are extensible. You

can use any operation available in the vCenter Server API to customize vRealize Orchestrator workflows.

Using the vSphere Client

2

Use the vSphere Client to connect to vCenter Server systems and manage vSphere inventory objects.

Use of the vSphere Client requires a supported Web browser.

The home screen of the vSphere Client is a system dashboard that aggregates data from different sources in the environment together in a single, unified view.

Overview of the vSphere Client Home Screen (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_homescreen)

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

Table 2-1. Supported Guest Operating Systems and Browser Versions for the vSphere Client.

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Edge: 79 or later.
	Mozilla Firefox: 60 or later.
	Google Chrome: 75 or later.
Mac OS	Microsoft Edge: 79 or later.
	Mozilla Firefox: 60 or later.
	Google Chrome: 75 or later.

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

This chapter includes the following topics:

- Log In to vCenter Server by Using the vSphere Client
- Manage the Login Message to the vSphere Client Login Page
- Navigate the vSphere Inventory by Using the Global Inventory Lists Navigator
- Manage Client Plug-Ins
- Install the VMware Enhanced Authentication Plug-in
- Refresh Data

- Searching the Inventory

- Sort the vSphere Client Inventory

- Drag Objects

- Export Lists

- Attach File to Service Request

- Keyboard Shortcuts

- Provide Feedback with the vSphere Client

- Start, Stop, and Restart Services

Log In to vCenter Server by Using the vSphere Client

You can use the vSphere Client to log in to vCenter Server and manage your vSphere inventory.

The vSphere Client is automatically 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`

    As an alternative, you can open a Web browser and enter the URL for the vSphere Client:
    `https://vcenter_server_ip_address_or_fqdn/ui`.

2   If a warning message about a potential security risk appears, select to continue to the website.

Browser	Action
Microsoft Edge	a Click **Details**.
	b Under the additional message that appears, click **Go on to the webpage**.
Mozilla Firefox	a Click **Advanced**.
	b Under the additional message that appears, click **Accept the Risk and Continue**.
Google Chrome	a Click **Advanced**.
	b Under the additional message that appears, click **Proceed to** *vcenter_server_ip_address_or_fqdn*.

3   On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.

4   If the warning message about a potential security risk appears again, repeat Step 2.

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

Results

The vSphere Client connects to all the vCenter Server systems on which the specified user has permissions, and you can view and manage the vSphere inventory.

Manage the Login Message to the vSphere Client Login Page

You can add a login message to the vSphere Client login page. You can also configure a custom login message and provide a check box for user consent.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Configuration UI.

   a   From the **Home** menu, select **Administration**.

   b   Under **Single Sign On**, click **Configuration**.

4 Click the **Login Message** tab.

5 Click **Edit** and configure the login message.

Option	Description
Show login message	Toggle on **Show login message** to enable the login message. You cannot make changes to the login message unless you toggle on this switch.
Login message	Title of the message. By default, when **Consent checkbox** is toggled on, the login message text is `I agree to Terms and Conditions`. You must replace `Terms and Conditions` with your own text. If the **Consent checkbox** is toggled off, then `Login message` appears, over which you enter your message.
Consent checkbox	Toggle on **Consent checkbox** to require that the user clicks a check box before logging in. You can also display a message without a check box.
Details of login message	Message that the user sees when clicking the login message, for example, the text of the terms and conditions. You must enter some details in this text box.

6 Click **Save**.

Navigate the vSphere Inventory by Using the Global Inventory Lists Navigator

You can use the **Global Inventory Lists** navigator to browse and select objects in the vSphere inventory as an alternative to the hierarchical inventory tree.

Unlike the inventory tree, which presents hierarchical arrangements of parent and child objects arranged in the **Hosts and Clusters**, **VMs and Templates**, **Storage**, and **Networking** inventory lists, the Global Inventory Lists navigator presents a list of all related objects in the inventory. You can navigate from an object to its related objects, regardless of their type.

Procedure

1 From the vSphere Client home page, click **Global Inventory Lists**.

2 In the left pane, select one of the object or resource categories to view objects of that type.

   For example, click **Hosts** to view the hosts in the vSphere inventory.

3 In the left navigation pane, click an object from the list once to display information about the object.

4 (Optional) Click the object again to open it.

   Opening an object brings it to the top of the navigator and displays related object categories beneath it.

   For example, opening a host allows you to see the child resource pools, virtual machines, datastores, networks, and distributed switches associated with this host.

5 To access additional information or manage the selected object, click one of the tabs in the center pane.

Option	Description
Summary	You can view basic status and configuration for an object.
Monitor	You can view alarms, performance data, resource allocation, events, and other status information for an object.
Configure	Depending on the selected object, you can edit settings, alarm definitions, tags, permissions, and so on.
Permissions	You can view, add, change, and delete permissions. This tab is only available for logged in users with administration privileges.
Related Objects tabs	You can view and manage the objects related to the object that you selected. For example, if you select a host, the tabs that you see are **VMs**, **Resource Pools**, **Datastores**, and **Networks**.
Updates	Depending on the selected object, you can check the hardware compatibility of a host against the VMware Compatibility Guide, check the status of virtual machines, upgrade the VMware Tools version or the virtual hardware version of the virtual machines, and perform vSphere Lifecycle Manager operations. **Note** The **Updates** tab is available only for certain types of inventory objects, for example, hosts, virtual machines, and clusters.

Manage Client Plug-Ins

With Client Plug-In Management you can monitor plug-in downloads, deployments, upgrades, and undeployments.

From the vSphere Client, you can monitor vCenter Server client plug-ins using the **Recent Tasks** pane, the global **Tasks** view, or the **Administration > Client Plugins** view. In addition to monitoring installation progress, you can troubleshoot installation failures and plug-in incompatibilities. You can also enable and disable installed plug-ins.

Monitor Client Plugins

You can monitor plug-in activities including installation progress, failures, deployments, upgrades, and undeployments. You can also enable or disable client plug-ins.

Procedure

1   In the vSphere Client home page, click **Administration > Solutions > Client Plugins**.

    The Client Plugins Table shows detailed plug-in information, including version, enablement status, and deployment status.

2   (Optional) To see more information about failed or incompatible deployments, click the status message.

3   (Optional) Enable or disable a client plug-in.

    a   Select the radio button next to the plug-in.

    b   Click **Enable** or **Disable**.

    c   Click **Yes**.

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.

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).

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.

Refresh Data

You must manually refresh the data in the vSphere Client to see changes made to objects by other users during your session.

For performance reasons, the vSphere Client does not continuously refresh data on all objects in the inventory. All changes that you make during your current session are immediately reflected in the client user interface. Change made by other users or in other sessions are not reflected until you manually refresh the data.

Procedure

◆   To update all data in the current vSphere Client view, click the refresh icon ().

    The client view is updated.

Searching the Inventory

With the vSphere Client, you can search the inventory for objects that match specified criteria. You can search the inventories of all vCenter Server systems.

You can only view and search for inventory objects that you have permission to view.

Note If your permissions change while you are logged in, the search service might not immediately recognize these changes. To ensure that your search is performed with up-to-date permissions, log out of all your open sessions and log in again before you perform the search.

- Perform a Quick Search

  A quick search checks all types of objects for the specified search term within the name or other properties of the object.

- Save a Search

  You can save search queries in the vSphere Client so you can rerun, rename, or delete them later.

- Manage a Saved Search

  In the vSphere Client, you can rename, delete, or create a duplicate of a saved search query.

Perform a Quick Search

A quick search checks all types of objects for the specified search term within the name or other properties of the object.

Procedure

1 Enter the search term in the search box at the top of the vSphere Client window.

   Multiple search terms in a quick or simple search are treated as if they are connected by ORs. For example, searching for `example machine` finds all objects with names containing either "example" or "machine".

   The search results appear below the search box as you type. The number of items displayed is limited to 10.

2 (Optional) To run a saved search, click the saved search icon and select a saved search query.

3 (Optional) To display an item in the inventory, click the item from the drop-down list of the search results.

4 (Optional) To see more search results or more details about the search results, click the summary of the search results from the drop-down list of search results.

   a   (Optional) To display an object in the inventory, click the object in the search results page.

   The search results are listed in tables arranged by object type. For example, if a search finds hosts and virtual machines, the following tables appear: **Hosts**, which shows only host results and **Virtual Machines**, which shows only virtual machine results.

Save a Search

You can save search queries in the vSphere Client so you can rerun, rename, or delete them later.

Procedure

1 In a vSphere Client window, enter a query for a simple search in the search box.

2 Click the summary of the search results from the drop-down list with search results.

3 On the search results page, click **Save Search**.

4 Enter a name for the search query. Names must be lowercase with no spaces.

5 Click **Save**.

The search query you entered is saved. You can reload the query later and repeat the search.

Manage a Saved Search

In the vSphere Client, you can rename, delete, or create a duplicate of a saved search query.

Procedure

1 At the top of the vSphere Client window, click inside the search box.

2 Click the saved search icon and select a saved search query.

3 On the Search Results page, click **Actions** and select one of the options:

Option	Description
Save as	Creates a duplicate of the saved search query.
Rename	Renames the saved search query.
Delete	Deletes the saved search query.

4 Confirm the changes.

Sort the vSphere Client Inventory

You can use sortable columns and input filters to sort and find objects in your vSphere Client inventory that meet certain criteria.

You can sort list views by column. These list views can be selected in the **Global Inventory Lists** pane or found in search results.

From a list view, you can use the **Filter** field to filter objects.

For example, you can sort virtual machines by name, provisioned space, used space, and so on. You can filter them by name, state, status, and so on.

Procedure

1 In the vSphere Client home page, select **Global Inventory Lists**.

2 To open an object list view, select an object type from the list.

If objects from the selected type are not present in the inventory, a blank page appears.

3   (Optional) Click the column you want to sort objects by. You can click again on that column to reverse the sorting order.

4   Add or remove columns from the object list view:

    a   Click the arrow in the upper right corner of a column and select **Show/Hide Columns**.

    b   (Optional) To show columns in the object list view, select the columns from the default list.

    c   (Optional) To hide columns from the object list view, deselect the columns from the default list.

5   (Optional) To filter objects, enter your filtering parameter in the filter field above the object list table. For example, in the virtual machine list view, type `powered on` to filter for all virtual machines that are in a powered on state.

    A list of inventory objects that meet your filtering criteria are displayed in your selected sorting order.

What to do next

After you apply a filter to an object list, the filter is active during the login session. To clear the filtered list of inventory objects, delete the filter criteria from the the filter field.

Drag Objects

You can select an inventory object, and while holding the left mouse button you can drag it to another object. Drag is an alternative way to initiate operations that are available in the context menu, such as **Move To** and **Migrate**.

For completing some drag operations, you do not need to perform any additional actions. For completing others, you might have to go through a wizard.

Procedure

1   On the vSphere Client home page, select an inventory list.

    The inventory tree appears.

2   Select the object to move and drag it to a destination object.

    The mouse pointer changes depending on whether you can drop the object to the object you currently point to.

Table 2-2. Mouse Icons Indicating Possible Drag Operations

Icon	Description
▶️⊕	You can drop the object that you are dragging into this object.
▶️⊗	You cannot drop the object that you are dragging into this object.

3   Drop the object on the destination object.

    A task starts in the Recent Tasks pane.

4   If a wizard opens, follow the prompts to complete the drag operation.

Results

The object is moved to the destination object that you selected.

Export Lists

You can export the contents of an inventory list view to a CSV file.

Procedure

1   In the vSphere Client, click **Menu** and select **Global Inventory Lists**.

2   In the left pane, select one of the object or resource categories to view objects of that type.

For example, click **Hosts** to view the hosts in the vSphere inventory.

3   Click **Export** ( ) at the bottom right corner of a list view.

The Export List Contents dialog box opens and lists the rows and columns available for inclusion in the CSV file.

4   Select whether you want all rows or your current selection of rows to be listed in the CSV file.

5   Select the columns you want listed in the CSV file.

6   Click **Export**.

Attach File to Service Request

You can attach files, such as log files or screenshots, to VMware Service Requests directly from the vSphere Client.

Prerequisites

If you already have a Service Request ID with VMware, you can use the vSphere Client to upload the system log bundles directly to your service request.

Procedure

1   From the vSphere Client sidebar, click **Administration**.

2   In the Administration panel, under Support, click **Upload File to Service Request**.

3   Click the **Upload File to Service Request** button.

4   Enter the Service Request ID.

5   Click **Browse** and select the file to attach.

6   Click **Upload**.

Results

You can monitor the Recent Tasks pane to see when the upload is complete, or if an error occurred.

Keyboard Shortcuts

Keyboard shortcuts allow you to navigate quickly or perform a task in the vSphere Client.

Inventory Keyboard Shortcuts

With inventory keyboard shortcuts you can quickly navigate to different inventories in the vSphere Client.

Table 2-3. Inventory Keyboard Shortcuts

Keyboard Combination on a Windows machine	Keyboard Combination on a Mac machine	Action
Ctrl+Alt+Home	Control+Option+Home	Home
Ctrl+Alt+1	Control+Option+1	Shortcuts
Ctrl+Alt+2	Control+Option+2	Hosts and Clusters
Ctrl+Alt+3	Control+Option+3	VMs and Templates
Ctrl+Alt+4	Control+Option+4	Storage
Ctrl+Alt+5	Control+Option+5	Networking
Ctrl+Alt+6	Control+Option+6	Content Libraries
Ctrl+Alt+7	Control+Option+7	Workload Management
Ctrl+Alt+8	Control+Option+8	Global Inventory Lists
Ctrl+Alt+R	Control+Option+R	Refresh
Ctrl+Alt+S repeat twice	Control+Option+S repeat twice	Search

Provide Feedback with the vSphere Client

You can use the improved feedback tool in the vSphere Client to provide timely feedback to our developers.

Procedure

1   From the vSphere Client home screen, click the feedback icon in the top right corner.

2   Select the type of feedback you want to give and enter your feedback in the **Description** window.

3   (Optional) Provide an email address and screenshots or other images.

4   Click **Send**.

Start, Stop, and Restart Services

In the vSphere Client, you can start, stop, and restart services that are running on vCenter Server. You can restart services upon a configuration change or for suspected functional or performance issues.

Prerequisites

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

Procedure

1   Log in to the vCenter Server Management Interface.

- Log in to the vCenter Server Management Interface directly.

- In the vSphere Client home page, select **Administration > System Configuration**. Click a node from the list.

2   On the vCenter Server Management Interface home page, click **Services**.

3   Select a service from the service list.

4   From the top menu, click **Restart**, **Start**, or **Stop**.

Unavailable options are dimmed.

Note   Restarting the Content Library Service also restarts the Transfer Service and the OVF Service. The Content Library Service, the Transfer Service, and the OVF Service run on the same Tomcat server.

Submit Suggestions for New Features and Feature Requests Through the vSphere Ideas Portal

3

You can provide suggestions for new features or share feature requests through the vSphere Ideas portal. The vSphere Ideas portal is integrated with my.vmware.com and all users with valid Customer Connect accounts can access the portal.

The vSphere Ideas portal is public. When you publish new ideas and feature requests, consider whether you want to share personal data.

You can access the vSphere Ideas portal directly by going to https://vsphere.ideas.aha.io/ and entering a valid Customer Connect user name and password.

Alternatively, you can access the vSphere Ideas portal by using the vSphere Client.

Prerequisites

Verify that you have a valid Customer Connect account.

Procedure

1   On the vSphere Client home page, click the feedback icon in the top-right corner.

2   In the **Send Feedback** dialog box, click **Idea**.

3   Click **Visit ideas portal**.

    You are redirected to my.vmware.com and prompted to log in.

4   On the Customer Connect login page, enter a valid user name and password.

    You are redirected to https://vsphere.ideas.aha.io/ .

5   On the vSphere Ideas portal home page, click **Add a new idea**.

6   On the **Add a new idea** page, enter the details about your idea and click **Share idea**.

Results

Your idea appears in the **Recent** tab. All users of the vSphere Ideas portal can view, subscribe, vote, and comment on your idea.

Using Enhanced Linked Mode

4

Enhanced Linked Mode links multiple vCenter Server systems. With Enhanced Linked Mode, you can view and search across all linked vCenter Server systems. This mode replicates roles, permissions, licenses, and other key data across systems.

Enhanced Linked Mode provides the following features for vCenter Server:

- You can log in to all linked vCenter Server systems simultaneously with a single user name and password.

- You can view and search the inventories of all linked vCenter Server systems within the vSphere Client.

- Roles, permission, licenses, tags, and policies are replicated across linked vCenter Server systems.

To join vCenter Server systems in Enhanced Linked Mode, connect them to the same vCenter Single Sign-On domain.

Enhanced Linked Mode requires the vCenter Server Standard licensing level, and is not supported with vCenter Server Foundation or vCenter Server Essentials.

For more information about vCenter Enhanced Linked Mode, see the *vCenter Server Installation and Setup* guide.

Configuring the Customer
Experience Improvement Program

5

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

This chapter includes the following topics:

- Categories of Information That VMware Receives
- Join the Customer Experience Improvement Program in the vSphere Client

Categories of Information That VMware Receives

This product participates in VMware's Customer Experience Improvement Program ("CEIP").

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Join the Customer Experience Improvement Program in the vSphere Client

You can choose to join your vCenter Server to the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time. To leave and rejoin your host to the CEIP, see the vSphere Single Host Management - VMware Host Client documentation.

Prerequisites

Obtain the user name and password of the administrator account.

Procedure

1   From the vSphere Client login page, log in to vCenter Server by using the credentials of the administrator account.

2   On the vSphere Client home page, click **Administration**.

3   Under Deployment, click **Customer Experience Improvement Program**

4   Click **Join** to enable the CEIP or **Leave CEIP** to disable the Program.

Organizing Your Inventory

6

Plan how to set up your virtual inventory and consider how the virtual machines that it will support are going to be used and administered. A large vSphere implementation might contain several virtual data centers with a complex arrangement of hosts, clusters, resource pools, and networks. It might involve multiple vCenter Server systems connected using Enhanced Linked Mode. Smaller implementations might require a single virtual data center with a much less complex topology.

Here are the questions to answer as you create and organize an inventory of virtual objects:

- Will some virtual machines require dedicated resources?

- Will some virtual machines experience periodic spikes in workload?

- Will some virtual machines need to be administered as a group?

- Will some virtual objects require one set of system permissions, while other objects will require a different set of permissions?

- Do you want to use multiple vSphere Standard Switches, or you want to have a single vSphere Distributed Switch per data center?

- Do you want to use vMotion and Distributed Resource Management with certain virtual machines but not others?

The left pane of the vSphere Client displays your vSphere inventory. You can add and arrange objects in any way with the following considerations:

- The name of an inventory object must be unique with its parent.

- vApp names must be unique within the Virtual Machines and Templates view.

- System permissions are inherited and cascade. When you assign a system permission to an object in the inventory, the same permission propagates down the object hierarchy.

Tasks for Organizing Your Inventory

Populating and organizing your inventory involves the following activities:

- Creating data centers.

- Adding hosts to the data centers.

- Organizing inventory objects in folders.

- Setting up networking by using vSphere Standard Switches or vSphere Distributed Switches. To use services such as vMotion, TCP/IP storage, VMware vSAN™, and Fault Tolerance, set up VMkernel networking for these services. For more information, see *vSphere Networking*.

- Configuring storage systems and creating datastore inventory objects to provide logical containers for storage devices in your inventory. See *vSphere Storage*.

- Creating clusters to consolidate the resources of multiple hosts and virtual machines. You can enable vSphere HA and vSphere DRS for increased availability and more flexible resource management. See *vSphere Availability* for information about configuring vSphere HA, and *vSphere Resource Management* for information about configuring vSphere DRS.

- Creating resource pools to provide logical abstraction and flexible management of the resources in vSphere. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. See *vSphere Resource Management* for details.

This chapter includes the following topics:

- Create a Data Center

- Create a Folder

- Add a Host to a Folder or a Data Center

- Creating and Configuring Clusters

- Extend a Cluster

Create a Data Center

A virtual data center is a container for all the inventory objects required to complete a fully functional environment for operating virtual machines. You can create multiple data centers to organize groups of environments to meet different user needs. For example, you can create a data center for each organizational unit in your enterprise or create some data centers for high-performance environments and other data centers for less demanding environments.

Prerequisites

Required privileges:

- **Datacenter.Create datacenter**

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 Right-click the vCenter Server object and select **New Datacenter**.

3 (Optional) Enter a name for the data center and click **OK**.

What to do next

Add hosts, clusters, resource pools, vApps, networking, datastores, and virtual machines to the data center.

Create a Folder

You can use folders to group objects of the same type for easier management. For example, you can apply a common set of permissions to the folder and these permissions apply to all objects grouped in the folder.

A folder can contain other folders, or a group of objects of the same type. For example, one folder can contain both virtual machines and another folder that contains virtual machines, but it cannot contain both hosts and a folder that contains virtual machines.

Procedure

1 In the vSphere Client, select either a data center or another folder as a parent object for the folder that you want to create.

2 Right-click the parent object and click **New Folder**.

- If the parent object is a folder, the new folder is of the same type as the parent folder - it can contain only objects of the same type that the parent folder contains.

- If the parent object is a data center, you can create one of four types of folders: **Host and Cluster** folders, **Network** folders, **Storage** folders, and **VM and Template** folders.

3 Enter a name for the folder and click **OK**.

What to do next

Move objects into the folder by right-clicking the object and selecting **Move To**. Select the folder as the destination. You can also move an object by dragging it to the destination folder.

Add a Host to a Folder or a Data Center

You can add hosts under a data center object, a folder object, or a cluster object. If a host contains virtual machines, those virtual machines are added under the host in the inventory.

Prerequisites

- Verify that a data center or a folder exists in the inventory.

- Obtain the user name and password of the root user account for the host.

- Verify that hosts behind a firewall are able to communicate with the vCenter Server system and all other hosts through port 902 or another custom-configured port.

- Verify that all NFS mounts on the host are active.

- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.

- If you want to add a host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, verify that the vCenter Server instance is suitable for a large or an x-large environment.

Procedure

1   In the vSphere Client, navigate to a data center or folder within a data center.

2   Right-click the data center or folder and select **Add Host**.

3   Enter the IP address or the name of the host and click **Next**.

4   Enter administrator credentials and click **Next**.

5   Review the host summary and click **Next**.

6   License the host through one of the following methods.

- Assign an already existing license.

- Assign a new license.

    a   Click **Create New Licenses**. The Add Host wizard minimizes in Work in Progress and the New Licenses wizard appears.

    b   Enter or copy and paste the new license key from Customer Connect and click **Next**.

    c   Enter a new name for the license and click **Next**.

    d   Review the new license and click **Finish**.

7   In the Add Host wizard, click **Next**.

8   (Optional) Select a lockdown mode option to disable the remote access for the administrator account after vCenter Server takes control of this host and click **Next**.

9   (Optional) If you add the host to a data center or a folder, select a location for the virtual machines that reside on the host and click **Next**.

10 Review the summary and click **Finish**.

Results

A new task for adding the host appears in the Recent Tasks pane. It might take a few minutes for the task to complete.

Creating and Configuring Clusters

A cluster is a group of hosts. When a host is added to a cluster, the resources of the host become part of the resources of the cluster. The cluster manages the resources of all hosts that it contains.

Starting with vSphere 6.7, you can create and configure a cluster that is hyper-converged. The hyper-converged infrastructure collapses compute, storage, and networking on a single software layer that runs on industry standard x86 servers.

You can create and configure a cluster by using the simplified Quickstart workflow in the vSphere Client. On the **Cluster quickstart** page, there are three cards for configuring your new cluster.

Table 6-1. The cards initiating wizards for renaming and configuring a new cluster

Cluster Quickstart Workflow	Description
1. Cluster basics	You can edit the cluster name and enable or disable cluster services. The card lists the services you enabled.
2. Add hosts	You can add new ESXi hosts. After the hosts are added, the card shows the total number of hosts present in the cluster and displays health check validation for those hosts.
3. Configure cluster	You can configure network settings for vMotion traffic, review and customize cluster services. After the cluster is configured, the card provides details on configuration mismatch and reports cluster health results through the vSAN Health service.

The **Skip Quickstart** button prompts you to continue configuring the cluster and its hosts manually. To confirm exiting the simplified configuration workflow, click **Continue**. After you dismiss the **Cluster quickstart** workflow, you cannot restore it for the current cluster.

If you plan to enable vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), and the VMware vSAN features, you must create clusters.

Starting with vSphere 7.0, you can create a cluster that you manage with a single image. By using vSphere Lifecycle Manager images, you can easily update and upgrade the software and firmware on the hosts in the cluster. Starting with vSphere 7.0 Update 2, during cluster creation, you can select a reference host and use the image on that host as the image for the newly created cluster. For more information about using images to manage ESXi hosts and clusters, see the *Managing Host and Cluster Lifecycle* documentation.

Starting with vSphere 7.0 Update 1, vSphere Cluster Services (vCLS) is enabled by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters. For more information about vCLS, see vSphere Cluster Services (vCLS).

Create a Cluster

You create a new and empty cluster object by using the Quickstart workflow in the vSphere Client.

Starting with vSphere 7.0, the clusters that you create can use vSphere Lifecycle Manager images for host updates and upgrades.

A vSphere Lifecycle Manager image is a combination of vSphere software, driver software, and desired firmware with regard to the underlying host hardware. The image that a cluster uses defines the full software set that you want to run on the ESXi hosts in the cluster: the ESXi version, additional VMware-provided software, and vendor software, such as firmware and drivers.

The image that you define during cluster creation is not immediately applied to the hosts. If you do not set up an image for the cluster, the cluster uses baselines and baseline groups. Starting with vSphere 7.0 Update 2, during cluster creation, you can select a reference host and use the image on that host as the image for the newly created cluster. For more information about using images and baselines to manage hosts in clusters, see the *Managing Host and Cluster Lifecycle* documentation.

Prerequisites

- Verify that a data center, or a folder within a data center, exists in the inventory.

- Verify that hosts have the same ESXi version and patch level.

- Obtain the user name and password of the root user account for the host.

- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.

- To create a cluster that you manage with a single image, review the requirements and limitations information in the *Managing Host and Cluster Lifecycle* documentation.

Required privileges:

- **Host.Inventory.Create cluster**

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 Select a data center.

3 Right-click the data center and select **New Cluster**.

4 Enter a name for the cluster.

5 Select DRS, vSphere HA, or vSAN cluster features.

Option	Description

To use DRS with this cluster	a Slide the switch to the right to enable the DRS service.
	
	b (Optional) Click the info icon on the left to see the **Default Settings** for the DRS service. The default values are:
	
	  ■ Automation Level: Fully Automated Migration
	  ■ Threshold: 3

To use vSphere HA with this cluster	a Slide the switch to the right to enable the vSphere HA service. b (Optional) Click the info icon on the left to see the **Default Settings** for the vSphere HA service. You are present with the following default values: <table><tr><td>Host Monitoring:</td><td>Enabled</td></tr><tr><td>Admission Control:</td><td>Enabled</td></tr><tr><td>VM Monitoring:</td><td>Disabled</td></tr></table>
To use vSAN with this cluster	■ Slide the switch to the right to enable the vSAN service. For more information on vSAN, see Creating a vSAN Cluster in the *vSAN Planning and Deployment* documentation.

You can override the default values later on in the workflow.

6 (Optional) To create a cluster that you manage with a single image, select the **Manage all hosts in the cluster with a single image** check box.

For information about creating a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

7 Click **Next**.

8 Review the cluster details and click **Finish**.

The cluster appears in the vCenter Server inventory. The **Quickstart** service appears under the **Configure** tab.

9 (Optional) To rename your cluster and to enable or disable cluster services, click **Edit** in the **Cluster basics** card.

Results

You have created an empty cluster in the vCenter Server inventory.

What to do next

Add hosts to the cluster.

Add a Host to a Cluster

You can add new and existing ESXi hosts to the vCenter Server inventory.

You can also add hosts to a DRS cluster. For more information, see *vSphere Resource Management*.

When you add the first three hosts to the cluster, vSphere Cluster Services (vCLS) agent virtual machines are added by default to the cluster. A quorum of up to three vCLS agent virtual machines are required to run in a cluster, one agent virtual machine per host. For more information about vCLS, see vSphere Cluster Services (vCLS).

Prerequisites

- Verify that hosts have the same ESXi version and patch level.

- Obtain the user name and password of the root user account for the host.

- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.

- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.

- To add a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

Procedure

1 In the vSphere Client, navigate to a cluster within a data center.

2 On the **Configure** tab, select **Configuration > Quickstart**.

3 Click **Add** in the **Add hosts** card.

4 On the **Add hosts** page, add new or existing hosts to the cluster.

- Add hosts that are not part of the vCenter Server inventory.

  a Click the **New hosts** tab.

  b Populate the IP Address and credentials text boxes for those hosts.

  c (Optional) To add more new hosts, click the **Add Host** button.

  d (Optional) To reuse the credentials for all added hosts, select the **Use the same credentials for all hosts** check box.

- Add hosts that are managed by your vCenter Server instance and are in the same data center as your cluster.

  a Click the **Existing hosts** tab.

  b From the list, select the hosts that you want to add to the cluster.

5   Click **Next**.

The **Host summary** page lists all hosts that will be added to the cluster and related warnings.

Note   If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the **Security Alert** pop-up.

6   On the **Host summary** page, review the details of the added hosts and click **Next**.

7   (Optional) On the **Import Image** page, select the host whose image to use as the image for the cluster.

The **Import Image** page appears when you add hosts to a cluster managed with a single image. For information about adding a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

8   On the **Ready to complete** page, review the IP addresses or FQDN of the added hosts and click **Finish**.

Review the number of added hosts and the health check validation, performed by the vSAN Health service, in the **Add hosts** card.

9   (Optional) Click **Re-validate** to retrigger the validation of the hosts.

Note   If an error occurs, it is visible in the **Recent Tasks** pane only.

Results

All hosts are placed in maintenance mode and added to your cluster. You can manually exit the maintenance mode.

What to do next

Configure your cluster default settings through the Quickstart workflow.

Configure a Cluster

To configure the host networking settings on your host and to customize the cluster settings, start the **Configure cluster** wizard, part of the Cluster quickstart workflow.

Procedure

1   In the vSphere Client, navigate to a cluster.

2   On the **Configure** tab, select **Configuration > Quickstart**.

The **Cluster quickstart** page appears.

Note   To configure your cluster host networking and services manually by referring to different parts of the vSphere software, click the **Skip quickstart** button. If you dismiss the **Cluster quickstart** workflow, you cannot restore it, and you have to configure manually any hosts that you add to this cluster in the future.

3   In the **Configure hosts** card, select **Configure**.

4 On the **Distributed switches** page, configure the cluster networking.

Alternatively, you can select the `Configure networking settings later` check box to configure the default settings only for the cluster services and to hide all options that are related to host networking.

Caution After you select the `Configure networking settings later` check box, and complete the **Configure cluster** workflow, you cannot perform the networking configuration in the future by using the **Configure cluster** wizard.

---

a Specify the number of distributed switches to create from the drop-down menu.

Note You can select up to three distributed switches.

The selected distributed switches are configured as part of this workflow and all hosts in the cluster connect to them.

b Enter a unique name for each of the distributed switches you are about to create.

c (Optional) Click **Use Existing** to select an existing compatible distributed switch and an existing compatible distributed port group.

d To set up the vMotion network, select a distributed switch from the drop-down menu and assign a new default port group to it.

e In the **Physical adapters** section, for each physical network adapter (NIC), select the distributed switch name from the drop-down menu.

The new distributed switch must be assigned to at least one physical adapter.

Note If you are using an existing distributed switch, the physical adapter selection must match the current mapping of the distributed switch. Any variation results in an error.

This mapping of physical NICs to the distributed switches is applied to all hosts in this cluster.

f Click **Next**.

5 If the vSphere DRS feature is enabled on the cluster, configure the networking options in the vMotion traffic page.

a (Optional) Select the **Use VLAN** check box and enter an ID for the vMotion distributed port group.

b (Optional) Select a protocol type from the drop-down menu.

c Select an IP type from the drop-down menu.

d (Optional) Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.

If the IP address type is set to `DHCP`, these text boxes are dimmed.

6 Click **Next**.

The **Advanced options** page appears.

7 (Optional) If you enabled the vSphere HA feature during cluster creation, use the options in the **High Availability** section to enable or disable host failure monitoring, virtual machine monitoring, and admission control.

If you enable admission control, you can specify the failover capacity by number of hosts.

8 (Optional) If you enabled the vSphere DRS feature during cluster creation, the **Distributed Resource Scheduler** section is visible.

    a   Set the Automation level to `Fully Automated`, `Partially Automated` or `Manual`.

    b   Select one of the five migration settings from the Migration threshold drop-down menu.

9 In the **Host Options** section, configure the Lockdown mode, NTP server address, and host update preference.

    a   Select a lockdown mode from the drop-down menu.

    b   (Optional) Enter an NTP server address or FQDN.

        If you enter more than one NTP server addresses, separate them by using commas.

    c   (Optional) Select a host update option from the drop-down menu.

    The settings are applied across all hosts in this cluster.

10 (Optional) In the **Enhanced vMotion Capability** section, enable EVC and select the CPU model from the EVC mode drop-down menu.

11 Click **Next**.

The **Review** page appears.

12 Review the settings and select **Finish**.

The card closes, and the progress of the operation appears in the **Recent Tasks** pane.

Results

You have created a fully configured cluster in the vCenter Server inventory.

What to do next

Expand your cluster by using the **Add hosts** card.

Extend a Cluster

You extend a configured cluster by adding hosts to it with the **Cluster quickstart** workflow in the vSphere Client.

After you configure your cluster, you can scale it out by adding more hosts. Then, you specify the network configuration for the new hosts in the cluster. During the initial configuration of the cluster, if you postponed configuring the host networking, no configuration, as for the existing hosts, is applied to the newly added hosts.

Extend a Cluster Without Host Networking Configuration

You extend a cluster by adding hosts to that cluster. If you previously configured the cluster without setting up the host networking, the configuration of the existing hosts in the cluster is applied to the new hosts.

Prerequisites

- Verify that you have an existing cluster and hosts added to it.

- During the initial cluster configuration, select the `Configure networking settings later` check box. For more information, see Configure a Cluster.

- Verify that hosts have the same ESXi version and patch level.

- Obtain the user name and password of the root user account for the host.

- To add a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

Procedure

1   In the vSphere Client home page, navigate to **Home > Hosts and Clusters** and select a configured cluster.

2   Right-click the cluster and select **Add Hosts**.

    The **Add hosts** wizard appears.

3   On the **Add hosts** page, add new or existing hosts to the cluster.

    - Add hosts that are not part of the vCenter Server inventory.

        a   Click the **New hosts** tab.

        b   Populate the IP Address and credentials text boxes for those hosts.

        c   (Optional) To add more new hosts, click the **Add Host** button.

        d   (Optional) To reuse the credentials for all added hosts, select the **Use the same credentials for all hosts** check box.

    - Add hosts that are managed by your vCenter Server instance and are in the same data center as your cluster.

        a   Click the **Existing hosts** tab.

        b   From the list, select the hosts that you want to add to the cluster.

4 Click **Next**.

The **Host summary** page lists all hosts that will be added to the cluster and related warnings.

Note If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the **Security Alert** pop-up.

5 On the **Host summary** page, review the details of the added hosts and click **Next**.

6 (Optional) On the **Import Image** page, select the host whose image to use as the image for the cluster.

The **Import Image** page appears when you add hosts to a cluster managed with a single image. For information about adding a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

7 On the **Ready to complete** page, click **Finish**.

The **Extend Cluster Guide** page appears.

8 In the **Configure hosts** card, select **Configure**.

A pop-up window appears. It informs you that the configuration for the hosts that exist in the cluster is applied to the newly added hosts.

9 Select **Continue**.

Results

After successful validation, your newly added hosts are configured as the existing hosts in your cluster, and the **Configure** button in the **Configure hosts** card becomes inactive. You can only click **Re-validate** to verify the cluster configuration.

What to do next

Configure the host networking manually and add more hosts to the cluster.

Extend a Cluster with Host Networking Configuration

You extend a hyper-converged cluster by adding hosts and configuring their networking to match the cluster configuration.

Prerequisites

- Verify that you have an existing cluster and hosts added to it.

- In the initial cluster configuration, you configured the host networking.

- Verify that hosts have the same ESXi version and patch level.

- Obtain the user name and password of the root user account for the host.

- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.

9 If the vSphere DRS feature is enabled on the cluster, configure the networking options in the **vMotion traffic** page.

    a   (Optional) Select the **Use VLAN** check box and enter an ID for the vMotion distributed port group.

    b   (Optional) Select a protocol type from the drop-down menu.

    c   Select an IP type from the drop-down menu.

    d   (Optional) Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.

        If the IP address type is set to DHCP, these text boxes are dimmed.

10 Click **Next**.

     The **Review** page appears.

11 Review the settings and select **Finish**.

     The card closes, and the progress of the operation appears in the **Recent Tasks** pane.

Results

After successful validation, your newly added hosts are configured as the existing hosts in your cluster and the **Configure** button in the **Configure hosts** card becomes inactive. You can only click **Re-validate** to verify the cluster configuration.

What to do next

Add more hosts to the cluster.

vSphere Tags and Attributes

7

Tags and attributes allow you to attach metadata to objects in the vSphere inventory to make it easier to sort and search for these objects.

A tag is a label that you can apply to objects in the vSphere inventory. When you create a tag, you assign that tag to a category. Categories allow you to group related tags together. When you define a category, you can specify the object types for its tags, and whether more than one tag in the category can be applied to an object.

For example, if you wanted to tag your virtual machines by guest operating system type, you can create a category called `operating system`. You can specify that it applies to virtual machines only and that only a single tag can be applied to a virtual machine at any time. The tags in this category might be `Windows`, `Linux`, and `Mac OS`.

Tags and categories can span multiple vCenter Server instances:

- If multiple on-premises vCenter Server instances are configured to use Enhanced Linked Mode, tags and tag categories are replicated across all these vCenter Server instances.

- When you use Hybrid Linked Mode, tags and tag categories are maintained across your linked domain. That means the on-premises SDDC and the VMware Cloud on AWS SDDC share tags and tag attributes.

For vSphere Tags and Attributes, VMware Cloud on AWS supports the same set of tasks as an on-premises SDDC.

This chapter includes the following topics:

- Create, Edit, or Delete a Tag Category

- Create a Tag

- Edit or Delete a Tag

- Assign or Remove a Tag

- Add Permissions for Tags and Tag Categories

- Tagging Best Practices

- Custom Attributes

Create, Edit, or Delete a Tag Category

You use categories to group tags together and define how tags can be applied to objects. You create, edit, and delete a tag category from the vSphere Client.

You can create a tag category explicitly, as explained here, or as part of the tag creation process. Each tag has to belong to at least one tag category.

Procedure

1 In the vSphere Client, click **Menu > Tags & Custom Attributes**.

2 Click the **Tags** tab and click **Categories**.

3 Start the task that you want to perform.

Option	Description
Create a tag category	Click the **New Category** icon.
Edit a tag category	Select a category and click the **Edit Category** icon.
Delete a tag category	Select a category from the list and click the **Delete Category** icon.

4 Edit the category options.

Option	Description
Category Name	The category name must be unique to the currently selected vCenter Server system.
Description	You can provide text in the description to describe the purpose or use of the category.
Tags Per Object	■ If you select **One Tag**, you can apply only one tag from this category to an object. Use this option for categories whose tags are mutually exclusive. For example, if you have a category called Priority with tags High, Medium, and Low, then each object should have only one tag because an object can have only one priority. ■ If you select **Many tags**, you can apply more than one tag from the category to an object. Use this option for categories whose tags are not mutually exclusive. After you have set Tags Per Object, you can change from **One Tag** to **Many Tags**, but not from **Many Tags** to **One Tag**.
Associable Object Types	Select whether tags in this category can be assigned to all objects or only to a specific type of object, such as a virtual machine or a datastore. Changes to the associable object type are limited. ■ If you initially selected a single object type, you can later change the category to work for all object types. ■ If you initially selected All Objects, you cannot restrict the category later.

5 Click **OK** or **Yes** to confirm.

Create a Tag

You can use tags to add metadata to inventory objects. You can record information about your inventory objects in tags, and you can use the tags in searches.

For information about creating a tag category, see Create, Edit, or Delete a Tag Category.

Procedure

1 In the vSphere Client, select **Menu > Tags & Custom Attributes**.

2 Select the **Tags** tab and click **Tags**.

3 Click **New**.

4 In the **Create Tag** dialog box, enter a name for the tag.

5 Enter a description of the tag.

6 Specify the tag category.

- Select an existing category from the **Category** drop-down menu.

- Click **Create New Category** and select the newly created category.

7 Click **Create**.

Results

The tag appears in the list of tags.

Edit or Delete a Tag

In the vSphere Client, you can edit an existing tag or delete it when you no longer need it.

Procedure

1 In the vSphere Client home, select **Menu > Tags & Custom Attributes**.

2 Select the **Tags** tab and click **Tags**.

3 Select a tag from the list.

4 Select your task.

- To edit a tag, click **Edit** and confirm the operation.

  You can edit the name and description of the tag.

- To delete a tag, click **Delete** and confirm the operation.

Assign or Remove a Tag

After you create tags, you can apply or remove them as metadata to objects in the vCenter Server inventory.

Procedure

1 In the vSphere Client, navigate to an inventory tree.

2 Select an object from the list and click **Actions**.

3 From the drop-down menu, select **Tags and Custom Attributes**.

4 Select the required action.

- To assign a tag, select **Assign Tag**.

- To remove a tag, select **Remove tag**.

5 Select a tag from the list and confirm the operation.

In the **Assign Tag** dialog box, you can also create new tags with the **Add tag** button. For information about creating a tag, see Create a Tag.

Add Permissions for Tags and Tag Categories

You can manage the user privileges for working with tags and categories. The procedure for assigning permissions to tags is the same as the procedure for assigning permissions to tag categories.

When you create a tag, you can specify which users and groups can operate with that tag. For example, you can grant administrative rights only to administrators and set read-only permissions for all other users or groups. You must have vSphere administrator credentials to set and manage permissions for tags.

Permissions for tags work similar to permissions for vCenter Server inventory objects. For more information, see the *vSphere Security* documentation.

Procedure

1 In the vSphere Client, select **Menu > Tags & Custom Attributes**.

2 On the **Tags** tab, click the **Tags** or **Categories** button.

Depending on the button that you click, you see the list of tags or the list of tag categories.

3 Select an item from the list and click **Add Permission**.

4 In the **Add Permission** dialog box, select a domain from the drop-down menu.

5 Search for a user or a group to add.

6 Select a role to add from the drop-down menu.

7 To enable permission inheritance, select the **Propagate to children** check box.

8 Click **OK**.

Tagging Best Practices

Incorrect tagging can lead to replication errors. To avoid these errors, diligently follow best practices when tagging objects.

When working with tags in multiple node situations, expect replication delays between the nodes (generally 30 seconds to 2 minutes depending on your setup). Follow these best practices to avoid replication errors:

- After creating a tag, if you immediately assign that tag to a local object, assign it from the management node where you created the tag.

- After creating a tag, if you immediately assign that tag to a remote object, assign it from the management node to which the object is local. Depending on your environment setup, allow for replication time to propagate the new tag before you use the tag.

- Avoid simultaneously creating categories and tags from different management nodes before categories and tags across nodes can finish the replication process. If duplicate categories or tags are created from different nodes at the same time, the duplicates might not be detected and will appear. If you see these results, manually delete duplicates from one management node.

Custom Attributes

You can use custom attributes in the vSphere Client to assign user-specific values for each object of the custom attribute type.

After you create the attributes, set the value for the attribute on each virtual machine or managed host, as appropriate. This value is stored with vCenter Server and not with the virtual machine or managed host. Use the new attribute to filter information about your virtual machines and managed hosts. If you no longer need the custom attribute, remove it. A custom attribute is always a string.

For example, suppose that you have a set of products and you want to sort them by sales representative. Create a custom attribute for the sales person's name, Name. Add the custom attribute, Name, column to one of the list views. Add the appropriate name to each product entry. Click the column title Name to sort alphabetically.

The custom attributes feature is available only when you are connected to a vCenter Server system.

Add and Edit Custom Attributes

You can create custom attributes in the vSphere Client and associate the attribute with an object, such as a host, virtual machine, cluster, or network. You can also edit custom attributes.

After you create the attributes, set an appropriate value for the attribute on each virtual machine. This value is stored with vCenter Server and not with the virtual machine. Use the new attribute to filter your virtual machines. If you no longer need the custom attribute, remove it. A custom attribute is always a string.

For example, suppose that you have a set of products and you want to sort them by sales representative.

1   Create a Name custom attribute for the sales person's name.

2   Add the Name custom attribute column to one of the list views and add a name to each product entry.

3   You can now click the Name column to sort alphabetically by sales person.

Note   Tags and tag categories support a finer-grained mechanism for tagging your object. Consider using tags and tag categories instead of custom attributes.

Procedure

1   In the vSphere Client Home menu, select **Tags and Custom Attributes**.

2   Click **Custom Attributes**.

All currently defined custom attributes for vCenter Server are displayed.

3   Click **New**.

4   Enter the values for the custom attribute.

   a   Type the name of the attributes in the **Attribute** text box.

   b   Select the attribute type from the **Type** drop-down menu.

   c   Click **OK**.

After you have defined an attribute on an object, it is available to all objects of that type in the inventory. However, the value you specify is applied only to the currently selected object.

5   You can later edit a custom attribute.

   a   Select the attribute and click **Edit**.

   b   Change the Name.

   c   Change the type if it's available.

   d   Click **OK**.

Working with Tasks

8

vSphere tasks are activities and actions that occur on an object within the vSphere inventory.

This chapter includes the following topics:

- View Tasks
- Schedule Tasks

View Tasks

Tasks represent system activities that do not complete immediately, such as migrating a virtual machine. For example, powering off a virtual machine is a task. You can perform this task manually every evening, or you can set up a scheduled task to power off the virtual machine every evening .

You can view tasks that are associated with a single object or all objects in the vSphere Client. By default, the tasks list for an object also includes tasks performed on its child objects. You can filter the list by removing tasks performed on child objects and by using keywords to search for tasks.

If you are logged in to a vCenter Server system that is part of a Connected Group, a column in the task list displays the name of the vCenter Server system on which the task was performed.

Procedure

1 Navigate to an object in the inventory.

2 Click the **Monitor** tab, then click **Tasks**.

   The task list contains tasks performed on the object and detailed information, such as target, task status, initiator, and start/completion time of the task.

3 (Optional) To view related events for a task, select the task in the list.

Schedule Tasks

You can schedule tasks to run once in the future or multiple times, at a recurring interval.

The tasks you can schedule are listed in the following table.

Table 8-1. Scheduled Tasks

Scheduled Task	Description
Add a host	Adds the host to the specified data center or cluster.
Change the power state of a virtual machine	Powers on, powers off, suspends, or resets the state of the virtual machine.
Change cluster power settings	Enable or disable DPM for hosts in a cluster.
Change resource settings of a resource pool or virtual machine	Changes the following resource settings: ■ CPU – Shares, Reservation, Limit. ■ Memory – Shares, Reservation, Limit.
Check compliance of a profile	Checks that a host's configuration matches the configuration specified in a host profile.
Clone a virtual machine	Makes a clone of the virtual machine and places it on the specified host or cluster.
Create a virtual machine	Creates a new virtual machine on the specified host.
Deploy a virtual machine	Creates a new virtual machine from a template on the specified host or cluster.
Migrate a virtual machine	Migrate a virtual machine to the specified host or datastore by using migration or migration with vMotion.
Make a snapshot of a virtual machine	Captures the entire state of the virtual machine at the time the snapshot is taken.
Scan for Updates	Scans templates, virtual machines, and hosts for available updates. This task is available only when vSphere Lifecycle Manager is installed.
Remediate	Installs missing patches from the baselines selected for remediation on the hosts discovered during the scan operation and applies the newly configured settings. This task is available only when vSphere Lifecycle Manager is installed.

You create scheduled tasks by using the **Scheduled Task** wizard. For some scheduled tasks, this wizard opens the wizard used specifically for that task. For example, if you create a scheduled task that migrates a virtual machine, the **Scheduled Task** wizard opens the **Migrate Virtual Machine** wizard, which you use to set up the migration details.

Scheduling one task to run on multiple objects is not possible. For example, you cannot create one scheduled task on a host that powers on all virtual machines on that host. You must create a separate scheduled task for each virtual machine.

After a scheduled task runs, you can reschedule it to run again at another time.

Create a Scheduled Task

You can create scheduled tasks for operations that you want to run automatically once or at a recurring interval.

If the task to schedule is not available in the vSphere Client, use the vSphere API. See the vSphere SDK *Programming Guide*.

Caution   Do not schedule multiple tasks simultaneously on the same object. The results are unpredictable.

Prerequisites

Required privilege: **Schedule Task.Create tasks**

Procedure

1   In the vSphere Client, navigate to the object for which you want to schedule a task.

2   Select **Configure > Scheduled Tasks > New Scheduled Task**.

3   From the **New Scheduled Task** drop-down menu, select the task to schedule.

A wizard opens for the task with (scheduled) appended next to its name. The wizard contains a **Scheduling options** page, where you configure the scheduling options for the task. For example, to schedule taking a virtual machine snapshot, the **Take a VM Snapshot wizard (scheduled)** opens. In **Scheduling options**, you configure the scheduling options for the task, and in **Edit settings**, you enter the properties for the snapshot.

4   In the **Scheduling options** page, configure the required settings for the task.

a   Type a name and a description for the task.

b   Choose a frequency.

Table 8-2. Scheduler options

Option	Description
Once	Runs the scheduled task at the time selected.
After vCenter startup	Runs the task a specified number of minutes after startup.
Hourly	1 Type the repeat frequency. 2 Type the start date and time. 3 Type the end date and time. For example, to start a task at the half-hour mark of every fifth hour, type **5** hours and **30** minutes.
Daily	1 Type the repeat frequency. 2 Type the start date and time. 3 Type the end date and time. For example, to run the task at 2:30 pm every four days, type **4** and **2:30**.
Weekly	1 Type the repeat frequency. 2 Select the day of the week. 3 Type the start date and time. 4 Type the end date and time. For example, to run the task at 6 am every Tuesday and Thursday, type **1** week, **6 am**, and select **Tuesday** and **Thursday**.
Monthly	1 Type the repeat frequency. 2 Select the days by using one of the following methods. ■ Type a specific day of the month and the number of months. For example, the tenth day every five months. ■ Select **first**, **second**, **third**, **fourth**, or **last**, and select the day of the week and the number of months. **last** runs the task on the last week in the month that the day occurs. For example, if you select the last Monday of the month and the month ends on a Sunday, the task runs six days before the end of the month.

c   Set up email notifications and click **OK**.

5

Change or Reschedule a Task

After a scheduled task is created, you can change the schedule, frequency, and other attributes of the task. You can edit and reschedule tasks before or after they run.

Prerequisites

Required privilege:**Schedule Task.Modify**

Procedure

1 In the vSphere Client, navigate to the object for which you want to edit a scheduled task.

To view all scheduled tasks for a vCenter Server instance, navigate to that vCenter Server instance.

2 Select **Configure**, and select **Scheduled Tasks**.

3 Select a task from the list on the left and click **Edit**.

4 Right-click the task and select **Edit**.

5 Change the task attributes as necessary.

6 Click **Save**.

Remove a Scheduled Task

Removing a scheduled task removes all future occurrences of the task. The history associated with all completed occurrences of the task remains in the vCenter Server database.

Prerequisites

Required privilege:**Scheduled task.Remove**

Procedure

1 In the vSphere Client, navigate to the object for which you want to remove a scheduled task.

To view all scheduled tasks for a vCenter Server instance, navigate to that vCenter Server instance.

2 Select **Configure**, and select **Scheduled Tasks**.

3 Select a task from the list on the left and click **Remove**.

Configuring Hosts in vCenter Server

9

Before you set up your virtual environment and consider how the virtual machines that it will support are going to be used and administered, you should configure ESXihosts in vCenter Server. The configuration of ESXi hosts involves several tasks.

This chapter includes the following topics:

- Host Configuration
- Synchronizing Clocks on the vSphere Network

Host Configuration

Before you create virtual machines on your hosts, you must configure the hosts to ensure that they have correct licensing, network and storage access, and security settings.

For information on configuring a host, see the configuration information for the specific vSphere component in the *vSphere Security*documentation, the *vSphere Storage* documentation, and the *vSphere Networking* documentation.

Configure the Boot Device on an ESXi Host

On servers running ESXi, you can select the device that the server boots from.

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 Select a host in the inventory and click the **Configure** tab.

3 Under Hardware, select **Overview** and click the **Boot Options** button.

4 Select a boot device from the drop-down menu.

5 (Optional) To reboot immediately from the device you selected, select **Apply and Reboot on OK**.

If you do not select **Apply and Reboot on OK**, the new setting takes effect when the host reboots next.

6 Click **OK**.

Configure Agent VM Settings

You can configure the datastore and network settings for the ESX agent virtual machines that you deploy on a host.

An ESX agent is a virtual machine, or a virtual machine and a vSphere Installation Bundle (VIB), that extend the functions of an ESXi host to provide additional services that a vSphere solution requires.

For example, a solution might require a particular network filter or firewall configuration to function. A solution can use an ESX agent to connect to the vSphere Hypervisor and extend the host with functions specific to that solution. For example, the ESX agent can filter network traffic, act as a firewall, or gather other information about the virtual machines on the host.

When you configure the datastore and network settings for ESX agents on a host, all of the ESX agents that you deploy on the host use that datastore and network configuration.

Important   ESX agents are deployed only if you configure the network and datastore settings.

Procedure

1   Select a host in the vSphere Client inventory.

2   Click the **Configure** tab.

3   Under **Virtual Machines**, select **Agent VM Settings**.

The current settings for the ESX agents on the host, if any, appear.

4   Click **Edit**.

5   From the **Datastore** drop-down menu, select a datastore in which to deploy the ESX agent virtual machines.

6   From the **Network** drop-down menu, select a network to connect the ESX agents.

7   Click **OK**.

What to do next

For information about ESX agents and ESX Agent Manager, see *Developing and Deploying vSphere Solutions, vServices, and ESX Agents*.

Set Advanced Host Attributes

You can set advanced attributes for a host.

Caution   Changing advanced options is considered unsupported. Typically, the default settings produce the optimum result. Change the advanced options only when you get specific instructions from VMware technical support or a knowledge base article.

Procedure

1   Browse to the host in the vSphere Client.

2   Click the **Configure** tab.

3   Under **System**, click **Advanced System Settings**.

4   Click the **Edit** button.

5   Find the appropriate item and change the value.

6   Click **OK**.

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*.

Editing the Time Configuration Settings of a Host

To ensure precise timestamping of events and synchronization of the time between an ESXi host and the other components in the vSphere network, configure the time settings of the ESXi host manually or synchronize the time and date of the host with an NTP or PTP server.

Exact timestamping shows the precise sequence of events that occur in the vSphere network. Time synchronization between the components of the vSphere network can prevent authentication problems, and prevent firstboot from failing at different services.

Configure the Date and Time on a Host Manually

You can configure the date and time settings of the ESXi host manually. When you disable the NTP and the PTP clients, the manual time configuration becomes active.

Prerequisites

- Verify that the NTP client and the PTP client are disabled on the host.

Procedure

1   In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2   Select a host.

3   On the **Configure** tab, select **System > Time Configuration**.

4   In the **Manual Time Configuration** pane, click **Edit**.

    The **Edit Manual Time Configuration** dialog box appears.

5   Enter a date and time and click **OK**.

Use NTP Servers for Time and Date Synchronization of a Host

To avoid time synchronization problems between an ESXi host and other components in the vSphere network, you can synchronize the time and date of the host to an NTP server.

The NTP and the PTP services cannot run simultaneously. Disable the PTP service and then enable the NTP service. Additionally, when you enable the NTP service, the manual time configuration becomes inactive.

Note   You can set an NTP service startup policy to control the start and stop of the NTP service. You can also change the NTP service status manually. For more information about services, see Change the NTP and PTP Service Status on the Host Manually .

Prerequisites

- Verify that the PTP client is disabled.

Procedure

1   In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2   Select a host.

3   On the **Configure** tab, select **System > Time Configuration**.

4   In the **Network Time Protocol** pane, click **Edit**.

5   In the **Edit Network Time Protocol** dialog box, edit the network time protocol settings.

a   Select **Enable**.

b   In the **NTP Servers** text box, enter the IP addresses or host names of the NTP servers that you want to use.

c   (Optional) To start the NTP service immediately, select the **Start NTP Service** check box.

d   From the **NTP Service Startup Policy** drop-down menu, select an option for starting and stopping the NTP service on the host.

Option	Description
Start and stop with port usage	Starts the NTP service when an NTP client port is enabled. Stops the NTP service when all ports are closed.
Start and stop with host	Starts and stops the NTP service when the host powers on and shuts down.
Start and stop manually	You must manually control the status of the NTP service.

e   Click **OK**.

Use PTP Servers for Time and Date Synchronization of a Host

To ensure that the time of an ESXi host is synchronized with the time of other components of the vSphere network, you can synchronize the time and date of the host to a PTP server.

The PTP and the NTP services cannot run simultaneously. Disable the NTP service and then enable the PTP service. Additionally, when you enable the PTP service, the manual time configuration becomes inactive.

Prerequisites

- Verify that the NTP client is disabled.

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 Select a host.

3 On the **Configure** tab, select **System > Time Configuration**.

4 In the **Precision Time Protocol** pane, click **Edit**.

5 In the **Edit Precision Time Protocol** dialog box, edit the precision time protocol settings.

   a Select **Enable**.

   b From the **Network interface** drop-down menu, select a network interface.

6 Click **OK**.

What to do next

Start the PTP service manually, see Change the NTP and PTP Service Status on the Host Manually .

Change the NTP and PTP Service Status on the Host Manually

You can manually start, stop, or restart the NTP or PTP service that runs on the host. In this way, you override the configured startup policy for the respective service.

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 Select a host.

3 On the **Configure** tab, select **System > Services**.

4 Change the status of the NTP or PTP service.

Option	Description
Option	Action
Change the NTP service status	a Select **NTP Daemon**. b Click **Start**, **Stop**, or **Restart**.
Change the PTP service status	a Select **PTP Daemon**. b Click **Start**, **Stop**, or **Restart**.

Managing Hosts in vCenter Server

10

To monitor all hosts in your virtual environment from one place and to simplify host configuration, connect the hosts to a vCenter Server system.

For information about configuration management of ESXi hosts, see the *vSphere Networking* documentation, the *vSphere Storage* documentation, and the *vSphere Security* documentation.

This chapter includes the following topics:

- Disconnecting and Reconnecting a Host
- Relocate a Host
- Remove a Host from vCenter Server
- Reboot or Shut Down an ESXi Host
- Verifying SSL Certificates for Legacy Hosts

Disconnecting and Reconnecting a Host

You can disconnect and reconnect a host that a vCenter Server system manages. Disconnecting a managed host does not remove it from vCenter Server, but temporarily suspends all monitoring activities that vCenter Server performs.

The managed host and its associated virtual machines remain in the vCenter Server inventory. By contrast, removing a managed host from vCenter Server deletes the managed host and all its associated virtual machines from the vCenter Server inventory.

If an ESXi host becomes disconnected due to a loss of network connectivity to vCenter Server, the ESXi host reconnects automatically to vCenter Server after network connectivity is restored. If you manually disconnect an ESXi host, see Reconnect a Managed Host for more information.

Reconnecting an ESXi host automatically or manually does not impact the running virtual machines, unless the host is part of a cluster and there are resource pool privileges configured.

Disconnect a Managed Host

Use the vSphere Client to disconnect a managed host from vCenter Server.

Procedure

1 Navigate to **Home > Hosts and Clusters** and select a host.

2 Right-click the host and select **Connection** > **Disconnect** from the pop-up menu.

3 In the confirmation dialog box that appears, click **Ok**.

If the managed host is disconnected, the word "disconnected" is appended to the object name in parentheses, and the object is dimmed. All associated virtual machines are similarly dimmed and labeled.

Reconnect a Managed Host

Use the vSphere Client to reconnect a managed host to a vCenter Server system.

Procedure

1 Navigate to **Home > Hosts and Clusters** and select a host.

2 Right-click the host and select **Connection** > **Connect** from the pop-up menu.

When the managed host's connection status to vCenter Server is changed, the statuses of the virtual machines on that managed host are updated to reflect the change.

Reconnecting Hosts After Changes to the vCenter Server SSL Certificate

vCenter Server uses an SSL certificate to encrypt and decrypt host passwords stored in the vCenter Server database. If the certificate is replaced or changed, vCenter Servercannot decrypt host passwords, and therefore cannot connect to managed hosts. If vCenter Server fails to decrypt a host password, the host is disconnected from vCenter Server.

You must reconnect the host and supply the login credentials, which are encrypted and stored in the database using the new certificate.

Relocate a Host

You can move a host to another location within the vSphere inventory by dragging the host to the new location. The new location can be a folder, a cluster, or you can place the host as a standalone object in the data center.

When a host is moved from a cluster to another destination in the vSphere inventory, the resources which the host provides are deducted from the total cluster resources. You can either keep the virtual machines in the same cluster and migrate them to other hosts, or keep them on the host and remove them from the cluster. For information about removing a host from a cluster, see the *vSphere Resource Management* documentation.

Prerequisites

Power off all virtual machines that are running on the host, or migrate the virtual machines to a new host by using vMotion.

Procedure

1   In the vSphere Client home page, navigate to **Home > Hosts and Clusters** and select a host.

2   If the host is part of a cluster, put it in maintenance mode.

    a   Right-click the host and select **Maintenance Mode > Enter Maintenance Mode**.

    b   (Optional) If the host is part of a DRS cluster, evacuate the powered off or suspended virtual machines to other hosts within the cluster by selecting the check box **Move powered-off and suspended virtual machines to other hosts in the cluster**.

    c   In the confirmation dialog box, click **OK**.

       The host enters maintenance mode.

3   Select the host in the vSphere inventory panel and drag it to the new location within the inventory.

4   Right-click the host and select **Maintenance Mode > Exit Maintenance Mode**.

5   (Optional) Power on the virtual machines that you powered off before you put the host in maintenance mode.

Remove a Host from vCenter Server

Remove a managed host from vCenter Server to stop vCenter Server from monitoring and managing that host.

If possible, remove managed hosts while they are connected. Removing a disconnected host does not remove the vCenter Server agent from the managed host.

Prerequisites

- Make sure that NFS mounts are active. If NFS mounts are unresponsive, the operation fails.

- If the host you want to remove from the cluster is connected to a distributed switch, remove the host from the switch. For more information, see Remove Hosts from a vSphere Distributed Switch in the *vSphere Networking* documentation.

Procedure

1   In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2   2. Select a host in the inventory.

3 (Optional) If the host is part of a cluster, put it in maintenance mode.

   a   Right-click the host and select **Maintenance Mode > Enter Maintenance Mode** from the pop-up menu.

      If not all virtual machines on the host are powered off, the host does not enter maintenance mode.

      If the host is part of a DRS cluster, when the host enters maintenance mode, DRS attempts to evacuate powered on virtual machines from the host by using vMotion.

   b   In the confirmation dialog box, click **Ok**.

      If the host is part of a DRS cluster, you can evacuate powered off or suspended virtual machines to other hosts within the cluster. Select the check box **Move powered-off and suspended virtual machines to other hosts in the cluster**.

      The host icon changes and the term Maintenance Mode is added to the name in parentheses.

4 Right-click the host you want to remove in the inventory pane, and select **Remove from Inventory** from the pop-up menu.

5 In the confirmation dialog box, click **Yes** to remove the host.

   vCenter Server removes the host and the associated virtual machines from the vCenter Server instance. vCenter Server then returns the status of all associated processor and migration licenses to available.

Reboot or Shut Down an ESXi Host

You can power off or restart any ESXi host using the vSphere Client. Powering off a managed host disconnects it from vCenter Server, but does not remove it from the inventory.

Procedure

1 Locate the ESXi host in the inventory.

2 Power off all virtual machines that run on the ESXihost.

3 Select the ESXi host you want to power off.

4 Select **Actions > Power**.

5 Select the operation.

   ■   To power off and restart the ESXi host, click **Reboot**.

   ■   To power off the ESXi host, click **Shut Down**.

6 Provide a reason for the operation and click **OK**.

   This information is added to the log.

Verifying SSL Certificates for Legacy Hosts

You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you configure this setting, vCenter Server and the vSphere Client check for valid SSL certificates before connecting to a host for operations such as adding a host or making a remote console connection to a virtual machine.

vCenter Server 5.1 and vCenter Server 5.5 always connect to ESXi hosts using SSL thumbprint certificates. Starting with vCenter Server 6.0, the SSL certificates are signed by VMware Certificate Authority by default. You can instead use certificates from a third-party CA. Thumbprint mode is supported only for legacy hosts.

Procedure

1   In the vSphere Client, navigate to the vCenter Server instance.

2   Select the **Configure** tab.

3   Under **Settings**, select **General**.

4   Click **Edit**.

5   Select **SSL settings**.

6   Determine the host thumbprint for each legacy host that requires validation.

   a   Log in to the direct console.

   b   Select **View Support Information** on the **System Customization** menu.

      The thumbprint is displayed in the column on the right.

7   Compare the thumbprint you obtained from the host with the thumbprint listed in the vCenter Server SSL settings dialog box.

8   If the thumbprints match, select the check box for the host.

   Hosts that are not selected will be disconnected after you click **Save**.

9   Click **Save**.

License Management

11

vSphere provides a centralized license management system that you can use to manage licenses for ESXi hosts, vCenter Server systems, vSAN clusters, Supervisor Clusters, and solutions. Solutions are products that integrate with vSphere such as VMware Site Recovery Manager, vCloud Networking and Security, vRealize Operations Manager, and others.

- **Licensing Terminology and Definitions**

  The licensing system in vSphere uses specific terminology and definitions to refer to different licensing-related objects.

- **The License Service in vSphere 7.0**

  In vSphere 7.0, the License Service is part of the vSphere environment. The License Service delivers centralized license management and reporting functionality to vSphere and to products that integrate with vSphere.

- **Licensing for Environments with vCenter Server Systems 6.0 and Later, and 5.5**

  If your vSphere 6.0 or later environment consists of vCenter Server 6.0 or later, and 5.5 systems, consider the differences in the license management and reporting between vSphere 6.0 and later, and vSphere 5.5.

- **Licensing for Products in vSphere**

  ESXi hosts, vCenter Server, vSAN clusters, and Supervisor Clusters are licensed differently. To apply their licensing models correctly, you must understand how the associated assets consume the license capacity. You must also understand how the evaluation period for each product works, what happens when a product license expires, and so on.

- **Suite Licensing**

  Suite products combine multiple components to provide a certain set of capabilities. Suite products have a single license that you can assign to all suite components. When participating in a suite, suite components have different licensing models than their standalone versions. Examples of suite products are vCloud Suite and vSphere with Operations Management.

- **Managing Licenses**

  To license an asset in vSphere, you must assign it a license that holds an appropriate product license key. You can use the license management functionality in the vSphere Client to license multiple assets at a time from a central place. Assets are vCenter Server systems, hosts, vSAN clusters, Supervisor Clusters, and solutions.

- **Viewing Licensing Information**

  You can view the licensing state of the vSphere environment from a central place by using the license management functionality in the vSphere Client . You can view the licenses that are available in vSphere, current license assignments and usage, available license capacity, licensed features in use, and so on.

- **Synchronizing Licenses with Your Customer Connect Account**

  With vSphere 6.5 and later, VMware offers the Synchronize Licenses feature that you can use to import license keys and license key data from Customer Connect to your vSphere environment.

- **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.

Licensing Terminology and Definitions

The licensing system in vSphere uses specific terminology and definitions to refer to different licensing-related objects.

License Key

A license key encodes details about the product it is associated with, the license expiration date, the license capacity, and other information. The license key is assigned to an object to activate the functionality of its associated product.

License

A container for a license key of a VMware product. To use a license key, you create a license object in the vSphere Client and insert the license key into the license. After the license is created, you can assign it to assets.

Product Edition

A set of specific features that are associated with a unique license key. When assigned, the license key unlocks the features in the product edition. Examples of product editions are vSphere Enterprise Plus, vSphere Standard, vCenter Server Essentials, and so on.

Feature

Enabled or disabled functionality by a license that is associated with a specific product edition. Examples of features are vSphere DRS, vSphere vMotion, and vSphere High Availability.

Solution

A product that is packed and distributed independently from vSphere. You install a solution in vSphere to take advantage of certain functionality. Every solution has a licensing model specific for the solution, but uses the License Service for license management and reporting. Examples of solutions are VMware Site Recovery Manager, vRealize Operations Manager, vCloud Network and Security, and so on.

Asset

Any object in vSphere that requires licensing. If the license has sufficient capacity, the license administrator in vSphere can assign one license to one or multiple assets of the same type. Suite licenses can be assigned to all assets that are part of the suite. Assets are vCenter Server systems, ESXi hosts, and products that integrate with vSphere such as VMware Site Recovery Manager, vRealize Operations Manager, and others.

License Capacity

The number of units that you can assign to assets. The units of a license capacity can be of different types depending on the product that the license is associated with. For example, a license for vCenter Server determines the number of vCenter Server systems that you can license.

License use

The number of units that an asset uses from the capacity of a license. For example, if you assign a per-virtual-machine license to VMware Site Recovery Manager, the license use for VMware Site Recovery Manager is the number of protected virtual machines.

The License Service in vSphere 7.0

In vSphere 7.0, the License Service is part of the vSphere environment. The License Service delivers centralized license management and reporting functionality to vSphere and to products that integrate with vSphere.

You can use the License Service with newly installed vSphere 6.0 and later environments. You can also use the License Service with environments that are upgraded from vSphere 5.x to vSphere 6.0 and later. For details about upgrading the license management in vCenter Server 5.x to the License Service in vSphere 6.0 and later, see the *vSphere Upgrade* guide.

The License Service provides an inventory of licenses in the vSphere environment, and manages the license assignments for ESXi hosts, vCenter Server systems, vSAN clusters, and Supervisor Clusters. The License Service also manages the license assignments for products that integrate with vSphere, such as vRealize Operations Manager, and VMware Site Recovery Manager.

If your vSphere environment has several vCenter Server systems that are joined in Enhanced Linked Mode, the licensing inventory is replicated across all linked vCenter Server systems. This way, the licensing data for each asset and all available licenses are replicated across all linked vCenter Server systems. Each individual vCenter Server system contains a copy of that data and licenses for all linked vCenter Server systems.

Note   Licensing data is replicated across multiple linked vCenter Server systems on a 10-minute interval.

For example, suppose that your environment consists of eight vCenter Server systems that are joined in Enhanced Linked Mode, and every vCenter Server system has 10 hosts connected to it. The License Service stores information about the license assignments and uses for all eight vCenter Server systems, and the 80 hosts that are connected to those systems. With the License Service, you can manage the licensing for all eight vCenter Server systems and the 80 hosts that are connected to them through the vSphere Client.

Licensing for Environments with vCenter Server Systems 6.0 and Later, and 5.5

If your vSphere 6.0 or later environment consists of vCenter Server 6.0 or later, and 5.5 systems, consider the differences in the license management and reporting between vSphere 6.0 and later, and vSphere 5.5.

The License Service in vSphere 6.0 and later manages the licensing data for all ESXi hosts, vSAN clusters, and solutions that are associated with the vCenter Server 6.0 and later systems in the vSphere environment. However, every standalone vCenter Server 5.5 system manages the licensing data only for the hosts, solutions, and vSAN clusters that are associated with that system. Licensing data for linked vCenter Server 5.5 systems is replicated only for the vCenter Server 5.5 systems in the group.

Due to the architectural changes in vSphere 6.0 and later, you can either manage the licensing data for all assets that are associated with all vCenter Server 6.0 and later systems in vSphere, or manage the licensing data for individual vCenter Server 5.5 systems or a group of linked vCenter Server 5.5 systems. The licensing interface in the vSphere Client allows you to select between all vCenter Server 6.0 and later systems and vCenter Server 5.5 systems.

Licensing for Products in vSphere

ESXi hosts, vCenter Server, vSAN clusters, and Supervisor Clusters are licensed differently. To apply their licensing models correctly, you must understand how the associated assets consume the license capacity. You must also understand how the evaluation period for each product works, what happens when a product license expires, and so on.

Licensing for ESXi Hosts

ESXi hosts are licensed with vSphere licenses. Each vSphere license has a certain capacity that you can use to license multiple physical CPUs on ESXi hosts.

Starting with vSphere 7.0, one CPU license covers one CPU with up to 32 cores. If a CPU has more than 32 cores, you need additional CPU licenses.

Number of CPUs	Cores per CPU	Number of CPU Licenses
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

When you assign a vSphere license to a host, the amount of capacity consumed is determined by the number of physical CPUs on the host and the number of cores in each physical CPU. vSphere Desktop that is intended for VDI environments is licensed on per virtual machine basis.

To license an ESXi host, you must assign it a vSphere license that meets the following prerequisites:

- The license must have sufficient capacity to license all physical CPUs on the host.

- The license must support all the features that the host uses. For example, if the host is associated with a vSphere Distributed Switch, the license that you assign must support the vSphere Distributed Switch feature.

If you attempt to assign a license that has insufficient capacity or does not support the features that the host uses, the license assignment fails.

If you use the licensing model with up to 32 cores, you can assign a vSphere license for 10 32-core CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts with 32 cores per CPU

- Five 1-CPU hosts with 64 cores per CPU

- Two 2-CPU hosts with 48 cores per CPU and two 1-CPU hosts with 20 cores per CPU

Dual-core and quad-core CPUs, such as Intel CPUs that combine two or four independent CPUs on a single chip, count as one CPU.

Evaluation Mode

After you install ESXi, it operates in evaluation mode for up to 60 consecutive days. An evaluation mode license provides all features of the highest vSphere product edition.

After you assign a license to an ESXi host, at any time before the evaluation period expires, you can set the host back to evaluation mode to explore the entire set of features available for the remaining evaluation period.

For example, if you use an ESXi host in evaluation mode for 20 days, then assign a vSphere Standard license to the host, and 5 days later set the host back to evaluation mode, you can explore the entire set of features available for the host for the remaining 35 days of the evaluation period.

License and Evaluation Period Expiry

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused before the license expiration.

Note   When there are expiring licenses, a notification appears 90 days before the license expiration.

Licensing ESXi Hosts After Upgrade

If you upgrade an ESXi host to a version that starts with the same number, you do not need to replace the existing license with a new one. For example, if you upgrade a host from ESXi 5.1 to 5.5, you can use the same license for the host.

If you upgrade an ESXi host to a major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade an ESXi host from 5.x to 6.x, you must license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license use for vSphere Desktop equals the total number of powered on desktop virtual machines running on the hosts that are assigned a vSphere Desktop license.

Licensing for vCenter Server

vCenter Server systems are licensed with vCenter Server licenses that have per-instance capacity.

To license a vCenter Server system, you need a vCenter Server license that has the capacity for at least one instance.

Evaluation Mode

When you install a vCenter Server system, it is in evaluation mode. An evaluation mode license of a vCenter Server system expires 60 days after the product is installed no matter whether you assign a license to vCenter Server or not. You can set vCenter Server back to evaluation mode only within 60 days after its installation.

For example, suppose that you install a vCenter Server system and use it in evaluation mode for 20 days and assign the system an appropriate license. The evaluation mode license of vCenter Server will expire after the remaining 40 days of the evaluation period.

License and Evaluation Period Expiry

When the license or evaluation period of a vCenter Server system expires, all hosts disconnect from that vCenter Server system. If after the license or evaluation period of vCenter Server expires that vCenter Server is assigned to a new license key, all disconnected hosts reconnect to the vCenter Server system.

Note   When there are expiring licenses, a notification appears 90 days before the license expiration.

Licensing vCenter Server After Upgrade

If you upgrade vCenter Server to a version that starts with the same number, you can keep the same license. For example, if you upgrade a vCenter Server system from vCenter Server 5.1 to 5.5., you can keep the same license on the system.

If you upgrade vCenter Server to a major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade a vCenter Server system from 5.x to 6.x, you must license the system with a vCenter Server 6 license.

If you upgrade the edition of the license, for example, from vCenter Server Foundation to vCenter Server Standard, replace the existing license on the system with the upgraded license.

Licensing for Clusters with vSAN Enabled

After you enable vSAN on a cluster, you must assign the cluster an appropriate vSAN license.

Similar to vSphere licenses, vSAN licenses have per CPU capacity. When you assign a vSAN license to a cluster, the amount of license capacity used equals the total number of CPUs in the hosts participating in the cluster. For example, if you have a vSAN cluster that contains 4 hosts with 8 CPUs each, assign the cluster a vSAN license with a minimum capacity of 32 CPUs.

The license use of the vSAN is recalculated and updated in one of the following cases:

- If you assign a new license to the vSAN cluster

- If you add a new host to the vSAN cluster

- If a host is removed from the cluster

- If the total number of CPUs in a cluster changes

You must maintain the vSAN clusters in compliance with the vSAN licensing model. The total number of CPUs of all hosts in the cluster must not exceed the capacity of the vSAN license that is assigned to the cluster.

License and Evaluation Period Expiry

When the license or the evaluation period of a vSAN expires, you can continue to use the currently configured vSAN resources and features. However, you cannot add SSD or HDD capacity to an existing disk group or create new disk groups.

vSAN for Desktop

vSAN for Desktop is intended for use in VDI environments, such as vSphere for Desktop or Horizon ™ View™. The license use for vSAN for Desktop equals the total number of powered on VMs in a cluster with enabled vSAN.

To remain EULA compliant, the license use for vSAN for Desktop must not exceed the license capacity. The number of powered on desktop VMs in a vSAN cluster must be less than or equal to the license capacity of vSAN for Desktop.

Licensing for vSphere with Tanzu

Once you configure a vSphere cluster for vSphere with Tanzu and it becomes a Supervisor Cluster, you must assign the cluster a Tanzu edition license before the 60 day evaluation period expires.

About the Tanzu Edition Licenses

A Tanzu edition license enables the Workload Management functionality in vSphere 7.0.1. It is applicable to Supervisor Clusters that are configured with the vSphere networking stack or with NSX-T Data Center as the networking stack.

As a vSphere administrator, when you assign a Tanzu edition license to a Supervisor Cluster cluster, you can create and configure namespaces and provide access to these namespaces to DevOps engineers. As a DevOps engineer, you can deploy Tanzu Kubernetes clusters and vSphere Pods inside the namespaces to which you have access. Supervisor Clusters configured with the vSphere networking stack only support Tanzu Kubernetes clusters.

Licensing a Supervisor Cluster

After you configure a vSphere clusters as a Supervisor Cluster, you can use the full set of capabilities of the cluster within a 60 day evaluation period. You must assign a Tanzu edition license to the Supervisor Cluster before the 60 day evaluation period expires.

If you configure NSX-T Data Center as the networking stack for the Supervisor Cluster, you must assign an NSX-T Data Center Advanced or higher license to NSX Manager.

If you upgrade an existing Supervisor Cluster to vSphere 7.0.1, the cluster enters evaluation mode after the upgrade completes. The VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license that is assigned to the hosts acts as a regular vSphere Enterprise 7 Plus license, it does not enable any vSphere with Tanzu functionality. In that case, you must assign the Supervisor Cluster a Tanzu edition license before the 60 day evaluation period expires.

Evaluation Period and Tanzu License Expiration

When the evaluation period of a Supervisor Cluster expires, or a Tanzu edition license expires, as a vSphere administrator you cannot create new namespaces or update the Kubernetes version of the Supervisor Cluster. As a DevOps engineer, you cannot deploy new vSphere Pods and Tanzu Kubernetes clusters. You cannot change the configuration of the existing Tanzu Kubernetes clusters such as adding new nodes.

You can still deploy workloads on Tanzu Kubernetes clusters and all existing workloads continue to run as expected. All Kubernetes workloads that are already deployed continue their normal operation.

Suite Licensing

Suite products combine multiple components to provide a certain set of capabilities. Suite products have a single license that you can assign to all suite components. When participating in a suite, suite components have different licensing models than their standalone versions. Examples of suite products are vCloud Suite and vSphere with Operations Management.

Licensing for VMware vCloud® Suite

VMware vCloud® Suite combines multiple components into a single product to cover the entire set of cloud infrastructure capabilities. When used together, the vCloud Suite components provide virtualization, software-defined data center services, policy-based provisioning, disaster recovery, application management, and operations management.

A vCloud Suite edition combines components such as vSphere, vCloud Director, vCloud Networking and Security, and others, under a single license. vCloud Suite editions are licensed on per-CPU basis. Many of the vCloud Suite components are also available as standalone products licensed on per-virtual machine basis. However, when these components are obtained through vCloud Suite, they are licensed on per-CPU basis.

The components from a vCloud Suite edition are activated with a single license key. For example, if you have a license key for vCloud Suite Standard, you assign the same key to all assets that will run vCloud Suite. For example, such assets include ESXi hosts, vCloud Automation Center, vCloud Director, and others.

All virtual machines running on a CPU licensed with a vCloud Suite edition can use all components included in that vCloud Suite edition. You can run unlimited number of virtual machines on the CPUs that are licensed with a vCloud Suite edition. To run virtual machines on CPUs that are not licensed for vCloud Suite, you need individual licenses for the products that you want to use.

For more information about the licensing model of vCloud Suite, see the vCloud Suite documentation.

Licensing for vSphere® with Operations Management

VMware vSphere® with Operations Management™ combines vSphere and vCenter™ Operations Management Suite™ Standard under a single suite with a single license. vSphere with Operations Management lets you gain operational insight in vSphere and optimize resource allocation by providing monitoring, performance, and capacity information about the vSphere environment.

vSphere with Operations Management is licensed on a per-CPU basis. To run vSphere with Operations Management, you must assign ESXi hosts a vSphere with Operations Management license. You can run unlimited number of virtual machines on the hosts that are licensed for vSphere with Operations Management.

Managing Licenses

To license an asset in vSphere, you must assign it a license that holds an appropriate product license key. You can use the license management functionality in the vSphere Client to license multiple assets at a time from a central place. Assets are vCenter Server systems, hosts, vSAN clusters, Supervisor Clusters, and solutions.

In vSphere, you can assign one license to multiple assets of the same type if the license has enough capacity. You can assign a suite license to all components that belong to the suite product edition. For example, you can assign one vSphere license to multiple ESXi hosts, but you cannot assign two licenses to one host. If you have a vCloud Suite license, you can assign the license to ESXi hosts, vCloud Networking and Security, vCenter Site Recovery Manager, and so on.

Managing Licenses in the vSphere Client
(http://link.brightcove.com/services/player/bcpid2296383276001?
bctid=ref:video_vsphere67_licenses)

Create New Licenses

When you purchase, divide, or combine license keys in Customer Connect, you must use the new keys to license assets in your vSphere environment. You must go to the vSphere Client and create a license object for every license key. A license is a container for a license key of a VMware product. After you create the new licenses, you can assign them to assets.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   On the **Licenses** tab, click **Add New Licenses**.

4   On the Enter licenses keys page, enter one license key per line, and click **Next**.

The license key is a 25-symbol string of letters and digits in the format XXXXX–XXXXX–XXXXX–XXXXX–XXXXX. You can enter a list of keys in one operation. A new license will be created for every license key that you enter.

5   On the Edit license names page, rename the new licenses as appropriate and click **Next** .

6   On the Ready to complete page, review the new licenses and click **Finish**.

Results

A new license is created for every license key that you entered.

What to do next

Assign the new licenses to hosts, vCenter Server systems, or other products that you use with vSphere. You must not keep unassigned licenses in the inventory.

Configuring License Settings for Assets in the vSphere Client

To continue using product functionality, you must assign appropriate licenses to assets in evaluation mode, or assets with expiring licenses. When you upgrade a license edition, combine, or split licenses in Customer Connect, you must assign the new licenses to assets. You can assign licenses that are already available or create licenses and assign them to the assets in a single workflow. Assets are vCenter Server systems, ESXi hosts, vSAN clusters, Supervisor Clusters, and other products that integrate with vSphere.

Assign a License to Multiple Assets

To continue using product functionality, you must assign appropriate licenses to assets in evaluation mode, or assets with expiring licenses. When you upgrade a license edition, combine, or split licenses in Customer Connect, you must assign the new licenses to assets. You can assign licenses that are already available, or create licenses and assign them to the assets in a single workflow. Assets are vCenter Server systems, ESXi hosts, vSAN clusters, Supervisor Clusters, and other products that integrate with vSphere.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   Select the **Assets** tab.

4   On the **Assets** tab, click the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or **Solutions** tab.

5   Select the assets to license.

   Note   Use Shift+click to select multiple assets.

6   Click **Assign License**.

7 In the **Assign License** dialog box, select the task that you want to perform.

◆ In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
Select a newly created license	a Click the **New License** tab.
	b In the **Assign License** dialog box, type or copy and paste a license key and click **OK**.
	c Enter a name for the new license and click **OK**.
	Details about the product, product features, capacity, and expiration period appear on the page.
	d Click **OK**.
	e In the **Assign License** dialog box, select the newly created license, and click **OK**.

Results

The license is assigned to the assets. Capacity from the license is allocated according to the license use of the assets. For example, if you assign the license to 3 hosts with 4 CPUs each, the consumed license capacity is 12 CPUs.

Configure License Settings for an ESXi Host

You must assign a license to an ESXi host before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vSphere licenses in Customer Connect, you must assign the new licenses to ESXi hosts and remove the old licenses.

Prerequisites

▪ To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Navigate to the host in the inventory.

2 Select the **Configure** tab.

3 Under **Settings**, select **Licensing**.

4 Click **Assign License**.

5 In the **Assign License** dialog box, select the task that you want to perform.

◆ In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
Select a newly created license	a Click the **New License** tab. b In the **Assign License** dialog box, type or copy and paste a license key and click **OK**. c Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. d Click **OK**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

Results

The license is assigned to the host. Capacity from the license is allocated according to the license use of the host.

Configure License Settings for vCenter Server

You must assign a license to a vCenter Server system before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vCenter Server licenses in Customer Connect, you must assign the new licenses to vCenter Server systems and remove the old licenses.

Prerequisites

■ To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 In the vSphere Client, navigate to the vCenter Server instance.

2 Select the **Configure** tab.

3 Under **Settings**, select **Licensing**.

4 Click **Assign License**.

5 In the **Assign License** dialog box, select the task that you want to perform.

◆ In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
Select a newly created license	a Click the **New License** tab. b In the **Assign License** dialog box, type or copy and paste a license key and click **OK**. c Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. d Click **OK**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

Results

The license is assigned to the vCenter Server system, and one instance from the license capacity is allocated for the vCenter Server system.

Configure License Settings for a vSAN Cluster

You must assign a license to a vSAN cluster before its evaluation period expires or its currently assigned license expires.

If you upgrade, combine, or divide vSAN licenses, you must assign the new licenses to vSAN clusters. When you assign a vSAN license to a cluster, the amount of license capacity used equals the total number of CPUs in the hosts participating in the cluster. The license use of the vSAN cluster is recalculated and updated every time you add or remove a host from the cluster. For information about managing licenses and licensing terminology and definitions, see the *vCenter Server and Host Management* documentation.

When you enable vSAN on a cluster, you can use vSAN in evaluation mode to explore its features. The evaluation period starts when vSAN is enabled, and expires after 60 days. To use vSAN, you must license the cluster before the evaluation period expires. Just like vSphere licenses, vSAN licenses have per CPU capacity. Some advanced features, such as all-flash configuration and stretched clusters, require a license that supports the feature.

Prerequisites

■ To view and manage vSAN licenses, you must have the **Global.Licenses** privilege on the vCenter Server systems.

Procedure

1 Navigate to your vSAN cluster.

2 Click the **Configure** tab.

3 Right-click your vSAN cluster, and choose menu Assign License.

4   Select an existing license and click **OK**.

Assign the Tanzu Edition License to a Supervisor Cluster

If you are using a Supervisor Cluster in evaluation mode, you must assign the cluster a Tanzu edition license before the 60 day evaluation period expires.

Note   If the evaluation period of a Supervisor Cluster expires, or the Tanzu edition license expires, as a vSphere administrator you cannot create any new namespaces on the Supervisor Cluster, or update the Kubernetes version of the cluster. As a DevOps engineer, you cannot create new vSphere Pods and Tanzu Kubernetes clusters. You cannot update the configuration of the existing Tanzu Kubernetes clusters, such as adding new nodes. All Kubernetes workloads that are already deployed continue their normal operation and you can deploy new workloads on the existing Tanzu Kubernetes clusters.

Procedure

1   In the vSphere Client, navigate to the Supervisor Cluster.

2   Select **Configure** and under **Licensing** select **Supervisor Cluster**.

3   Select **Assign License**.

4   In the **Assign License** dialog, click **New License**.

5   Enter a valid license key and click **OK**.

Set Assets to Evaluation Mode

To explore the complete set of features available for an asset, you can set it to evaluation mode.

Different products have different terms for using their evaluation mode. Before you set an asset to evaluation mode, you should consider the specifics for using the evaluation mode of its associated product. For details, see the licensing model documentation for the relevant product at Licensing for Products in vSphere.

Prerequisites

■   To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   Select the **Assets** tab.

4   Select the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or **Solutions** tab.

5   Select the asset that you want to set to evaluation mode.

6   Click the **Assign License** icon.

7   Select **Evaluation License** and click **OK** to save your changes.

Results

The asset is in evaluation mode. You can explore the entire set of features that are available for the asset.

Note   You must assign an appropriate license to the asset before its evaluation period expires. Otherwise the asset gets into unlicensed state and certain functionality will be blocked.

Rename a License

After you create a license, you can change its name.

Prerequisites

■   To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   Select the **Licenses** tab.

4   Select the license to rename, and click **Rename License**.

5   Type the new license name and click **OK**.

Remove Licenses

To remain in compliance with the licensing models of products that you use with vSphere, you must remove all unassigned licenses from the inventory. If you have divided, combined, or upgraded licenses in Customer Connect, you must remove the old licenses.

For example, suppose that you have upgraded a vSphere license from 6.7 to 7.0 in Customer Connect. You assign the license to ESXi 7.0 hosts. After assigning the new vSphere 7.0 licenses, you must remove the old vSphere 6.7 license from the inventory.

Prerequisites

■   To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   Select the **Licenses** tab.

4 Use the filters to display only the unassigned licenses.

5 Click the filter icon (▾) in the **State** column.

A text box appears.

6 Select what licenses you want to display (unassigned or assigned).

7 Select a license to remove or press Ctrl+A to select all licenses.

8 Click **Remove Licenses**, review the confirmation message, and click **Yes**.

Viewing Licensing Information

You can view the licensing state of the vSphere environment from a central place by using the license management functionality in the vSphere Client . You can view the licenses that are available in vSphere, current license assignments and usage, available license capacity, licensed features in use, and so on.

You can also export information about licenses and their expiration dates, capacity, and usage. You can export data about the available products and assets in the vSphere Client by downloading a `.`CSV file.

Managing Licenses in the vSphere Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_licenses)

View Licensing Information About the vSphere Environment

You can view the available licenses in vSphere and their expiration dates, available capacity, and usage. You can also view the available products and assets.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Select a tab for the licensing information that you want to view.

Tab	Description
Licenses	Lists all licenses that are available in the vSphere environment. For every license, you can view the associated license key, license usage, license capacity, and expiration date.
Products	Lists the products that have licenses available in the vSphere environment. You can view the licenses that are available for every product, licensed features, license usage, and license capacity.
Assets	Displays licensing information about the assets that are available in the vSphere environment. Assets are vCenter Server systems, hosts, vSAN clusters, Supervisor Clusters, and other products that you use with vSphere that are listed under Solutions.

What to do next

If you have upgraded, divided, or combined any licenses in Customer Connect, you must not use these old license keys and should remove them from the inventory.

View Available Licenses and Features About a Product

You can view information about a product, such as the available licenses, features, and license capacity in the vSphere Client.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Click the **Products** tab and select the product for which you want to view information.

4 Select the task that you want to perform.

Task	Description
View the licenses that are available for the selected product	In the vSphere Client, click the **Licenses** subtab below the list of products.
View the licensed features for the product	In the vSphere Client, click the **Features** subtab below the list of products.

View the Features That an Asset Can Use

You can view the features that an asset can use based on the license that is assigned to it.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Select the **Assets** tab.

4 Select the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or the **Solutions** option.

5 Select an asset and view the associated features.

6 Click the **Features** subtab below the list of assets.

View the License Key of the License

In vSphere, a license holds a license key for a product. You can view the associated license key for every license.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Select the **Licenses** tab.

4 Select a license from the list and view the license key.

5 Click the **Summary** subtab that is below the list of licenses. Under General, you can see the license name, the expiration date, the state of the license, and the license key.

View the Licensed Features for an Asset

Before you start to use a feature on an asset, you can check whether the asset is licensed to use this feature. For example, to use vSphere HA, you must check whether all hosts in a vSphere HA cluster are licensed for this feature.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Navigate to the vCenter Server system, host, or cluster whose licensed features you want to view.

2 Click the **Configure** tab.

3 Under Settings, select **Licensing**.

Results

The list of features that you can configure on the asset appears on the right.

Export Licensing Information in the vSphere Environment

You can export licensing information about vSphere licenses, products, or assets. The information is saved on your local system as a `.CSV` file. You can later open the `.CSV` file with third-party applications.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 (Optional) Select an item to export.

- Click the **Licenses** tab to select one or more licenses to export.

- Click the **Products** tab to select a product to export.

- Click the **Assets** tab to select the vCenter Server instance, hosts, clusters, or solutions whose licensing information you want to export.

If you do not select a particular license, product, or asset, all items from the respective list are exported.

Option	Description
vSphere Client	a (Optional) If you select an asset, specify the asset information to export by using the **Filter** ( ) icon below the list of assets. b To export the selected item or items, click **Export > Selected Rows**. c To export all items of the respective type, click **Export > All Rows**. d Click **OK** to save the file on your local system.

Synchronizing Licenses with Your Customer Connect Account

With vSphere 6.5 and later, VMware offers the Synchronize Licenses feature that you can use to import license keys and license key data from Customer Connect to your vSphere environment.

The Synchronize Licenses feature helps you keep your vCenter Server license keys data synchronized with the license keys data in Customer Connect. To import license keys data, you use a .CSV file that you generate in the Customer Connect reports section. After you import the .CSV file, you can view the Customer Connect data in the License List and the License Summary.

With the import feature, you can complete the following tasks:

- Add or update Customer Connect license keys details, such as notes, custom labels, contracts, orders, and so on, in your vCenter license inventory.

- Add license keys from Customer Connect to your vCenter license inventory.

- Identify any license keys in your vCenter license inventory that have been combined, divided, upgraded, or downgraded in Customer Connect to help you with license compliance.

Managing Licenses in the vSphere Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_licenses)

Synchronize Licenses

Use the Synchronize Licenses feature to import license key data from your Customer Connect account to your vSphere environment.

Prerequisites

Generate a Products, Licenses, Details, and History report in your Customer Connect account and upload it to vSphere. See Generate a CSV File in Customer Connect.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Follow the prompts in the **Synchronize Licenses** wizard.

    a   On the **Licenses** tab, click **Synchronize Licenses**.

        The **Synchronize Licenses** wizard opens.

    b   On the Upload import file page, click **select a file** and browse to the `.CSV` file that you want to upload in your vSphere environment. Click **Next**.

        After you upload the `.CSV` file to your vSphere environment, the system analyzes the data in the file and compares the data to the current license keys information in your vCenter license inventory. Based on the results of the analysis, the system concludes what actions you must perform to update your vCenter license inventory with the current details from your Customer Connect environment.

        Note Do not open in Microsoft Excel or any other software the `.CSV` file that you plan to upload to your vCenter license inventory. Upload only the original `.CSV` file after you generate it in Customer Connect. If you want to preview the report data in the `.CSV` file, make a copy of the file and preview the copy instead. For information how to preview CSV files, see Using CSV Files .

    c   On the License keys data analysis, review the results from the `.CSV` file analysis and click **Next**.

        For information about the types of actions that the system might recommend you to perform based on the `.CSV` file analysis, see Previewing the Results of the CSV File Analysis.

        If the `.csv` file contains license keys that are missing from the vCenter license inventory, the system offers you to add those license keys.

    d   (Optional) On the Add license keys page, select license keys to add to the vCenter Server license inventory.

        ■   If your vCenter license inventory contains all license keys in the uploaded `.CSV` file, click **Next**.

            If your vCenter license inventory contains all license keys in the uploaded `.CSV` file, the list on the Add License Keys page is empty.

        ■   To view license key details, such as account name and number, order number, important dates, and support level, click a license key in the list.

        ■   To change the license key name, click the license's name in the list and enter a new name for the license key.

    e   (Optional) To remove license keys in your vCenter license inventory that have been combined, split, upgraded, or downgraded in Customer Connect, download the `Combined_Split_Upgraded_and_Downgraded_License_Keys.csv` report. For information how to remove manually license keys that have been combined, split, upgraded, or downgraded, see Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded.

f   (Optional) To upgrade license keys in your vCenter license inventory that have upgrade keys available in Customer Connect, download the `Upgraded_License_Keys.csv` report. For information how to upgrade your assets manually, change your license assignments, and remove the upgraded license keys, see Upgrade License Keys in Your vCenter License Inventory.

g   On the Ready to complete page, review the import process summary and click **Finish**.

Generate a CSV File in Customer Connect

To update your vCenter license inventory with the license keys details in your Customer Connect environment, generate a Products, Licenses, Details, and History `.CSV` file in your Customer Connect reports section. Upload the `.CSV` file to vSphere.

The `.CSV` file is a list of keys that are active keys in Customer Connect. The `.CSV` file contains up-to-date license keys information from your Customer Connect environment, including the account name and number, the product for which the license is purchased, the license quantity, various license key notes, the support level, the license support and license coverage end date, the order number, history data, and so on.

Procedure

1   Log in to https://my.vmware.com.

2   On the Customer Connect home page, click **Products and Accounts** in the top left corner.

3   Select **Accounts** and click **Reports**.

4   In the **Select a Report** section, click **Available Reports** and select **Products and Licenses Details** from the drop down menu.

5   In the **Select Accounts** section, select the account, for which you want to generate the report or select the check box .

6   (Optional) Enter a name for your report.

7   (Optional) Add notes to include in your report.

8   (Optional) To receive an email when the report is ready, select the **Send email when report is created** check box **All Accounts** to select all available accounts.

9   Click **Create** and click **OK**.

Your report request is submitted and when the report is ready, you can download it from the list of saved reports.

10   To download the `.CSV` file that you must import to vSphere, in the **Saved Reports** section, click the CSV icon next to your report.

Do not change the formatting of the original `.CSV` file report. For information how to preview the `.CSV` file report and view the data without damaging the `.CSV` file, see Using CSV Files .

Previewing the Results of the CSV File Analysis

To determine what actions you must perform in order to update your vCenter license inventory with the current details from your Customer Connect environment, review the results from the .CSV file analysis.

After you upload the .CSV file that you generated in Customer Connect to your vSphere environment, the system analyzes the license keys in that .CSV file and compares them to the licenses in your vCenter license inventory. The following events occur as a result of the analysis:

- If the .CSV report contains licenses, which are missing in the vCenter license inventory, the analysis automatically offers to add the missing licenses to the vCenter license inventory.

- The system updates the vCenter licenses metadata after you finish the **Synchronize Licenses** wizard, to ensure that your vCenter license inventory contains the most up-to-date metadata from Customer Connect.

- If the system determines that your vCenter license inventory contains licenses that are invalid or upgraded, or both, the system proposes actions that you can take to update your vCenter license inventory at the last page of the **Synchronize Licenses** wizard.

Based on the conclusions from the analyzed data, the system proposes actions that you must perform in order to update your vCenter license inventory with details from your Customer Connect environment. You can view the conclusions from the analysis on the File analysis page of the **Synchronize Licenses** wizard.

Depending on the results from the.CSV file analysis, the system makes conclusions about the status of the license keys details in your vCenter license inventory and might suggest that you perform some of the following actions, in order to update your vSphere environment with up-to-date license keys details from Customer Connect:

- Update license keys in your vCenter license inventory with details from your Customer Connect, including contracts, orders, and so on. The system performs this operation automatically after you complete the wizard.

- Add to your vCenter license inventory new license keys from Customer Connect, and their details. You must perform this operation manually. To select license keys to add to your vCenter license inventory, follow the prompts in **Synchronize Licenses** wizard. See Synchronize Licenses.

  Note   Some of the license keys that you add might be replacement keys for inactive keys that are currently in your vCenter license inventory. An inactive key is a key that is combined, divided, upgraded, or downgraded. To complete the replacement of inactive license keys with new license keys from Customer Connect, you must manually remove the inactive keys. For information about removing inactive license keys, see Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded.

  Other license keys that you add on the Add license keys page of the wizard might be upgrade keys for some old license keys in your vCenter license inventory. To complete the upgrade process of old keys in your vCenter license inventory with new keys from Customer Connect, you must manually remove the inactive keys. For information about completing the license key upgrade process, see Upgrade License Keys in Your vCenter License Inventory.

- View license keys in your vCenter license inventory that have been combined, split, upgraded, or downgraded in Customer Connect. To view the keys that have been combined, split, upgraded, or downgraded, download the generated recommendation report at the end of the **Synchronize Licenses** wizard.

- Upgrade the keys in your vCenter license inventory that have upgrade keys available in Customer Connect. To view what keys in your vCenter license inventory have upgrade keys available in Customer Connect, download the generated recommendation report at the end of the **Synchronize Licenses** wizard.

Using CSV Files

If you want to preview the data in a `.CSV` file before you import the file to vSphere, make a copy of the `.csv` file. Do not open the original file in Microsoft Excel as this action might change the data formats of certain cells, which might cause issues in future releases.

If you attempt to import a `.csv` file that you first open in another program, the **Synchronize Licenses** wizard displays a warning that the file you use is not in the correct format, and that some of the data might not be available in vSphere.

Even if you successfully import the `.csv` file after you reformat it, the reformatting might corrupt the data, which might cause the last page of the wizard suggest some invalid actions.

Example: Incorrect Use of a CSV File

You export the correct report in Customer Connect and generate the correct `.csv` file. To view the information more clearly, you open the `.csv` file in Microsoft Excel and reformat dates and numbers, such as the contract start and end date, the order date, the order quantity. For instance, you change the formatting of the date from `11.10.2015` to `10/11/15`, which might cause the UI to display missing data for some of the columns of the `.csv` file.

Using Generated Recommendation Reports

After you import the `.CSV` file that you generate in the Customer Connect reports section to your vCenter license inventory, the system analyzes the license keys details in that `.CSV` file and compares the information with the information in your current vSphere environment. Based on the results from the `.CSV` file analysis, the system might generate recommendation reports that you can download and use to update your vSphere license inventory manually.

Note The recommendation reports are only available on the Ready to complete page of the **Synchronize Licenses** wizard. Download the reports to perform the actions manually.

For information how to remove from your vSphere license inventory existing license keys that have been combined, divided, upgraded, or downgraded in Customer Connect, see Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded.

For information how to upgrade your assets manually, change your license assignments, and remove license keys from your vCenter license inventory that have upgrade keys available in Customer Connect, see Upgrade License Keys in Your vCenter License Inventory.

Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded

If you have existing license keys in your vCenter license inventory that are combined, divided, upgraded, or downgraded in Customer Connect, use the generated recommendation `Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv` report to remove these license keys manually.

When you add license keys to your vCenter license inventory that the system proposes on the Add license keys page of the **Synchronize Licenses** wizard, and after you complete the wizard, you update your vCenter license inventory with new license keys and license keys that are replacement for some inactive keys in your vCenter license inventory. An inactive key is a key that is combined, divided, upgraded, or downgraded. To complete the replacement of inactive keys with new keys from Customer Connect, you must manually remove the keys that the `Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv` report indicates as inactive.

Prerequisites

Verify that you have the `Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv` report that is only available to download on the Ready to complete page of the **Synchronize Licenses** wizard.

Procedure

1 Click **Menu > Administration**.

2 Expand **Licensing** and click **Licenses**.

3 Select the **Licenses** tab.

4 Open your `Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv` file and locate the **Inactive Key in Use in vCenter** column.

5   View the inactive key in the `.CSV` file, select that same key in the **Licenses** tab in the vSphere Client, click the **Remove Licenses** icon, and click **Yes**.

You can only remove a license if it is not assigned.

The inactive license key is no longer in your vCenter license inventory and the inventory now only contains up-to-date keys from Customer Connect.

What to do next

To use product features, assign the licenses to assets after you add your license keys to your vCenter license inventory.

Upgrade License Keys in Your vCenter License Inventory

If you have existing license keys in your vCenter license inventory that have upgrade keys available in Customer Connect, use the generated recommendation `.CSV` file report to upgrade your assets manually, change your license assignments, and remove the outdated keys from your vCenter license inventory.

When you add license keys to your vCenter license inventory that the system proposes on the Add license keys page of the **Synchronize Licenses** wizard, and after you complete the wizard, you update your vCenter license inventory with new license keys that must upgrade some old keys in your vCenter license inventory. To complete the upgrade process for the old keys in your vCenter license inventory with new keys from Customer Connect, you must manually remove the keys that the `Upgraded_License_Keys.csv` report indicates as inactive.

Prerequisites

Verify that you have the `Upgraded_License_Keys.csv` report that is only available to download on the Ready to complete page of the **Synchronize Licenses** wizard.

Procedure

1   Click **Menu > Administration**.

2   Expand **Licensing** and click **Licenses**.

3   Select the **Licenses** tab.

4   Open your `Upgraded_License_Keys.csv` file and locate the **Inactive Key in Use in vCenter** column.

5   View the inactive key in the `.CSV` file, select that same key in the **Licenses** tab in the vSphere Client, click the **Remove Licenses** icon, and click **Yes**.

You can only remove a license if it is not assigned.

The license key is no longer in your vCenter license inventory.

What to do next

To use product features, assign the licenses to assets after you add your license keys to your vCenter license inventory.

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.

For more information about cross-domain repointing, see "Repoint vCenter Server to Another vCenter Server in a Different Domain" in *vCenter Server Installation and Setup*.

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. For instructions on how to remove the licenses in vCenter Server, see Remove Licenses.

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 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 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 to create licenses and Assign a License to Multiple Assets 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.

Migrating Virtual Machines

<div style="text-align: right">12</div>

You can move virtual machines from one compute resource or storage location to another by using cold or hot migration. For example, with vSphere vMotion you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to collocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

Moving a virtual machine from one inventory folder to another folder or resource pool in the same data center is not a form of migration. Unlike migration, cloning a virtual machine or copying its virtual disks and configuration file are procedures that create a new virtual machine. Cloning and copying a virtual machine are also not forms of migration.

By using migration, you can change the compute resource that the virtual machine runs on. For example, you can move a virtual machine from one host to another host or cluster.

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

Depending on the power state of the virtual machine that you migrate, migration can be cold or hot.

Cold Migration

Moving a powered off or suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one virtual switch to another, and from one data center to another. You can perform cold migration manually or you can schedule a task.

Hot Migration

Moving a powered on virtual machine to a new host. Optionally, you can also move the virtual machine disks or folder to a different datastore. Hot migration is also called live migration or vMotion. With vMotion, you migrate the virtual machine without any interruption in its availability.

Depending on the virtual machine resource type, you can perform three types of migration.

Change compute resource only

Moving a virtual machine, but not its storage, to another compute resource, such as a host, cluster, resource pool, or vApp. You can move the virtual machine to another compute resource by using cold or hot migration. If you change the compute resource of a powered on virtual machine, you use vMotion.

Change storage only

Moving a virtual machine and its storage, including virtual disks, configuration files, or a combination of these, to a new datastore on the same host. You can change the datastore of a virtual machine by using cold or hot migration. If you move a powered on virtual machine and its storage to a new datastore, you use Storage vMotion.

Change both compute resource and storage

Moving a virtual machine to another host and at the same time moving its disk or virtual machine folder to another datastore. You can change the host and datastore simultaneously by using cold or hot migration.

In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between the following types of objects.

Migrate to another virtual switch

Moving the network of a virtual machine to a virtual switch of a different type. You can migrate virtual machines without reconfiguring the physical and virtual network. By using cold or hot migration, you can move the virtual machine from a standard to a standard or distributed switch, and from a distributed switch to another distributed switch. When you move a virtual machine network between distributed switches, the network configuration and policies that are associated with the network adapters of the virtual machine are transferred to the target switch.

Migrate to another data center

Moving a virtual machine to a different data center. You can change the data center of a virtual machine by using cold or hot migration. For networking in the target data center, you can select a dedicated port group on a distributed switch.

Migrate to another vCenter Server system

Moving a virtual machine to a different vCenter Server instance.

You can move a virtual machine to a vCenter Server instance that is connected to the source vCenter Server instance through vCenter Enhanced Linked Mode.

You can also move virtual machines between vCenter Server instances that are located across a long distance from each other.

Starting with 7.0 Update 1c, you can migrate workloads across vCenter Server systems by using Advanced Cross vCenter vMotion. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

This chapter includes the following topics:

- Cold Migration
- Migration with vMotion
- Migration with Storage vMotion
- CPU Compatibility and EVC
- Migrate a Powered Off or Suspended Virtual Machine
- Migrate a Virtual Machine to a New Compute Resource
- Migrate a Virtual Machine to a New Compute Resource and Storage
- Migrate a Virtual Machine to New Storage
- Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host
- Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack
- Limits on Simultaneous Migrations
- About Migration Compatibility Checks

Cold Migration

Cold migration is the migration of powered off or suspended virtual machines between hosts across clusters, data centers, and vCenter Server instances. By using cold migration, you can also move associated disks from one datastore to another.

You can use cold migration to have the target host checked against fewer requirements than when you use vMotion. For example, if you use cold migration when a virtual machine contains a complex application setup, the compatibility checks during vMotion might prevent the virtual machine from moving to another host.

You must power off or suspend the virtual machines before you begin the cold migration process. Migrating a suspended virtual machine is considered a cold migration because although the virtual machine is powered on, it is not running.

You cannot implement a cold migration across different subnets.

CPU Compatibility Check During Cold Migration

If you attempt to migrate a powered off virtual machine that is configured with a 64-bit operating system to a host that does not support 64-bit operating systems, vCenter Server generates a warning. Otherwise, CPU compatibility checks do not apply when you migrate powered off virtual machines with cold migration.

When you migrate a suspended virtual machine, the new host for the virtual machine must meet CPU compatibility requirements. This requirement allows the virtual machine to resume execution on the new host.

Operations During Cold Migration

A cold migration consists of the following operations:

1   If you select the option to move to a different datastore, the configuration files, including the NVRAM file (BIOS settings), log files, and the suspend file, are moved from the source host to the destination host's associated storage area. You can choose to move the virtual machine's disks as well.

2   The virtual machine is registered with the new host.

3   After the migration is completed, the old version of the virtual machine is deleted from the source host and datastore if you selected the option to move to a different datastore.

Network Traffic for Cold Migration

By default, data for VM cold migration, cloning, and snapshots is transferred through the management network. This traffic is called provisioning traffic. It is not encrypted but uses run-length encoding of data.

On a host, you can dedicate a separate VMkernel network adapter to the provisioning traffic, for example, to isolate this traffic on another VLAN. On a host, you can assign no more than one VMkernel adapter for provisioning traffic. For information about enabling provisioning traffic on a separate VMkernel adapter, see the *vSphere Networking* documentation.

If you plan to transfer high volumes of virtual machine data that the management network cannot accommodate, redirect the cold migration traffic on a host to the TCP/IP stack that is dedicated to cold migration and cloning of powered off virtual machines. You can also redirect if you want to isolate cold migration traffic in a subnet different from the management network, for example, for migration over a long distance. See Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

Migration with vMotion

If you must take a host offline for maintenance, you can move the virtual machine to another host. Migration with vMotion™ allows virtual machine processes to continue working throughout a migration.

When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements so that the migration can proceed.

vMotion Migration Types

With vMotion, you can change the compute resource on which a virtual machine is running. You also can change both the compute resource and the storage of the virtual machine.

When you migrate virtual machines with vMotion and choose to change only the host, the entire state of the virtual machine is moved to the new host. The associated virtual disk remains in the same location on storage that must be shared between the two hosts.

When you choose to change both the host and the datastore, the virtual machine state is moved to a new host and the virtual disk is moved to another datastore. vMotion migration to another host and datastore is possible in vSphere environments without shared storage.

After the virtual machine state is migrated to the alternate host, the virtual machine runs on the new host. Migrations with vMotion are transparent to the running virtual machine.

When you choose to change both the compute resource and the storage, you can use vMotion to migrate virtual machines across vCenter Server instances, data centers, and subnets.

Transferred State Information

The state information includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes transaction data and the bits of the operating system and applications that are in the memory. The defining and identification information stored in the state includes all the data that maps to the virtual machine hardware elements. This information includes BIOS, devices, CPU, MAC addresses for the Ethernet cards, chipset states, registers, and so forth.

Stages in vMotion

Migration with vMotion occurs in three stages:

1   When the migration with vMotion is requested, vCenter Server verifies that the existing virtual machine is in a stable state with its current host.

2   The virtual machine state information (memory, registers, and network connections) is copied to the target host.

3   The virtual machine resumes its activities on the new host.

If errors occur during migration, the virtual machine reverts to its original state and location.

Host Configuration for vMotion

Before using vMotion, you must configure your hosts correctly.

Ensure that you have correctly configured your hosts.

■   Each host must be correctly licensed for vMotion.

- Each host must meet shared storage requirements for vMotion.

- Each host must meet the networking requirements for vMotion.

Important The ESXi firewall in ESXi 6.5 and later does not allow per-network filtering of vMotion traffic. Therefore, you must apply rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket on TCP port 8000.

---

vMotion Across Long Distances

You can perform reliable migrations between hosts and sites that are separated by high network round-trip latency times. vMotion across long distances is enabled when the appropriate license is installed. No user configuration is necessary.

For long-distance migration, verify the network latency between the hosts and your license.

- The round-trip time between the hosts must be up to 150 milliseconds.

- Your license must cover vMotion across long distances.

- You must place the traffic related to transfer of virtual machine files to the destination host on the provisioning TCP/IP stack. See Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

vMotion Shared Storage Requirements

Configure hosts for vMotion with shared storage to ensure that virtual machines are accessible to both source and target hosts.

During a migration with vMotion, the migrating virtual machine must be on storage accessible to both the source and target hosts. Ensure that the hosts configured for vMotion use shared storage. Shared storage can be on a Fibre Channel storage area network (SAN), or can be implemented using iSCSI and NAS.

If you use vMotion to migrate virtual machines with raw device mapping (RDM) files, make sure to maintain consistent LUN IDs for RDMs across all participating hosts.

See the *vSphere Storage* documentation for information on SANs and RDMs.

vSphere vMotion Networking Requirements

Migration with vMotion requires correctly configured network interfaces on source and target hosts.

Configure each host with at least one network interface for vMotion traffic. To ensure secure data transfer, the vMotion network must be a secure network, accessible only to trusted parties. Additional bandwidth significantly improves vMotion performance. When you migrate a virtual machine with vMotion without using shared storage, the contents of the virtual disk is transferred over the network as well.

vSphere 6.5 and later allow the network traffic with vMotion to be encrypted. Encrypted vMotion depends on host configuration, or on compatibility between the source and destination hosts.

Requirements for Concurrent vMotion Migrations

You must ensure that the vMotion network has at least 250 Mbps of dedicated bandwidth per concurrent vMotion session. Greater bandwidth lets migrations complete more quickly. Gains in throughput resulting from WAN optimization techniques do not count towards the 250-Mbps limit.

To determine the maximum number of concurrent vMotion operations possible, see Limits on Simultaneous Migrations. These limits vary with a host's link speed to the vMotion network.

Round-Trip Time for Long-Distance vMotion Migration

If you have the proper license applied to your environment, you can perform reliable migrations between hosts that are separated by high network round-trip latency times. The maximum supported network round-trip time for vMotion migrations is 150 milliseconds. This round-trip time lets you migrate virtual machines to another geographical location at a longer distance.

Multiple-NIC vMotion

You can configure multiple NICs for vMotion by adding two or more NICs to the required standard or distributed switch. For details, see Knowledge Base article KB 2007467.

Network Configuration

Configure the virtual networks on vMotion enabled hosts as follows:

- On each host, configure a VMkernel port group for vMotion.

  To have the vMotion traffic routed across IP subnets, enable the vMotion TCP/IP stack on the host. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host.

- If you are using standard switches for networking, ensure that the network labels used for the virtual machine port groups are consistent across hosts. During a migration with vMotion, vCenter Server assigns virtual machines to port groups based on matching network labels.

  Note By default, you cannot use vMotion to migrate a virtual machine that is attached to a standard switch with no physical uplinks configured, even if the destination host also has a no-uplink standard switch with the same label.

  To override the default behavior, set the `config.migrate.test.CompatibleNetworks.VMOnVirtualIntranet` advanced settings of vCenter Server to **false**. The change takes effect immediately. For details about the setting, see Knowledge Base article KB 1003832. For information about configuring advanced settings of vCenter Server, see *vCenter Server Configuration*.

For information about configuring the vMotion network resources, see Networking Best Practices for vSphere vMotion .

For more information about vMotion networking requirements, see Knowledge Base article KB 59232.

Networking Best Practices for vSphere vMotion

Consider certain best practices for configuring the network resources for vMotion on an ESXi host.

- Provide the required bandwidth in one of the following ways:

Physical Adapter Configuration	Best Practices
Dedicate at least one adapter for vMotion.	Use at least one 1 GbE adapter for workloads that have a small number of memory operations. Use at least one 10 GbE adapter if you migrate workloads that have many memory operations. If only two Ethernet adapters are available, configure them for security and availability. ■ For best security, dedicate one adapter to vMotion, and use VLANs to divide the virtual machine and management traffic on the other adapter. ■ For best availability, combine both adapters into a team, and use VLANs to divide traffic into networks: one or more for virtual machine traffic and one for vMotion
Direct vMotion traffic to one or more physical NICs that have high-bandwidth capacity and are shared between other types of traffic as well	■ To distribute and allocate more bandwidth to vMotion traffic across several physical NICs, use multiple-NIC vMotion. ■ On a vSphere Distributed Switch 5.1 and later, use vSphere Network I/O Control shares to guarantee bandwidth to outgoing vMotion traffic. Defining shares also prevents from contention as a result from excessive vMotion or other traffic. ■ To avoid saturation of the physical NIC link as a result of intense incoming vMotion traffic, use traffic shaping in egress direction on the vMotion port group on the destination host. By using traffic shaping you can limit the average and peak bandwidth available to vMotion traffic, and reserve resources for other traffic types. ■ In vSphere 7.0 Update 1 or earlier, vMotion saturates 1 GbE and 10 GbE physical NICs with a single vMotion VMkernel NIC. Starting with vSphere 7.0 Update 2, vMotion saturates high speed links such as 25 GbE, 40 GbE and 100 GbE with a single vMotion VMkernel NIC. If you do not have dedicated uplinks for vMotion, you can use Network I/O Control to limit vMotion bandwidth use.

- Provision at least one additional physical NIC as a failover NIC.

- Use jumbo frames for best vMotion performance.

    Ensure that jumbo frames are enabled on all network devices that are on the vMotion path including physical NICs, physical switches, and virtual switches.

- Place vMotion traffic on the vMotion TCP/IP stack for migration across IP subnets that have a dedicated default gateway that is different from the gateway on the management network. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host.

For information about configuring networking on an ESXi host, see the *vSphere Networking* documentation.

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

Encrypted vSphere vMotion secures confidentiality, integrity, and authenticity of data that is transferred with vSphere vMotion. vSphere supports encrypted vMotion of unencrypted and encrypted virtual machines across vCenter Server instances.

What Is Encrypted

For encrypted disks, the data is transmitted encrypted. For disks that are not encrypted, Storage vMotion encryption is not supported.

For virtual machines that are encrypted, migration with vSphere vMotion always uses encrypted vSphere vMotion. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines.

Encrypted vSphere vMotion States

For virtual machines that are not encrypted, you can set encrypted vSphere vMotion to one of the following states. The default is Opportunistic.

Disabled

Do not use encrypted vSphere vMotion.

Opportunistic

Use encrypted vSphere vMotion if source and destination hosts support it. Only ESXi versions 6.5 and later use encrypted vSphere vMotion.

Required

Allow only encrypted vSphere vMotion. If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

When you encrypt a virtual machine, the virtual machine keeps a record of the current encrypted vSphere vMotion setting. If you later disable encryption for the virtual machine, the encrypted vMotion setting remains at Required until you change the setting explicitly. You can change the settings using **Edit Settings**.

Note Currently, you must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances. See *vSphere Web Services SDK Programming Guide* and *vSphere Web Services API Reference*.

Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

vSphere vMotion supports migrating and cloning encrypted virtual machines across vCenter Server instances.

When migrating or cloning encrypted virtual machines across vCenter Server instances, the source and destination vCenter Server instances must be configured to share the key provider that was used to encrypt the virtual machine. In addition, the key provider name must be the same on both the source and destination vCenter Server instances. The destination vCenter Server ensures the destination ESXi host has encryption mode enabled, ensuring the host is cryptographically "safe."

The minimum version requirements for migrating or cloning encrypted virtual machines across vCenter Server instances using vSphere vMotion are:

- Both the source and destination vCenter Server instances must be on version 7.0 or later.

- Both the source and destination ESXi hosts must be on version 6.7 or later.

The following privileges are required when using vSphere vMotion to migrate or clone an encrypted virtual machine across vCenter Server instances.

- Migrating: **Cryptographic operations.Migrate** on the virtual machine

- Cloning: **Cryptographic operations.Clone** on the virtual machine

Also, the destination vCenter Server must have the **Cryptographic operations.EncryptNew** privilege. If the destination ESXi host is not in "safe" mode, the **Cryptographic operations.RegisterHost** privilege must also be on the destination vCenter Server.

Certain tasks are not allowed when migrating encrypted virtual machines across vCenter Server instances.

- You cannot change the VM Storage Policy.

- You cannot perform a key change.

vSphere Trust Authority and Encrypted vMotion

vSphere Trust Authority supports vSphere vMotion in migrating and cloning encrypted virtual machines across vCenter Server instances with the following requirements.

- The vSphere Trust Authority service must be configured for the destination host and the destination host must be attested.

- Encryption cannot change on migration. For example, an unencrypted disk cannot be encrypted while the virtual machine is migrated to the new storage.

- You can migrate a standard encrypted virtual machine onto a Trusted Host. The key provider name must be the same on both the source and destination vCenter Server instances.

- You cannot migrate a vSphere Trust Authority encrypted virtual machine onto a non-Trusted Host.

Enable or Disable Encrypted vMotion

You can enable encrypted vMotion during virtual machine creation. You can later change the encrypted vMotion state from the virtual machine settings. You can change the encrypted vMotion state only for virtual machines that are not encrypted.

For more information about virtual machine encryption, see Encrypted vSphere vMotion.

Prerequisites

Encrypted vMotion is supported only in vSphere 6.5 and later.

Procedure

1 Right-click the virtual machine and select **Edit Settings**.

2 Select **VM Options**.

3 Click **Encryption**, and select an option from the **Encrypted VMotion** drop-down menu.

Disabled

Do not use encrypted vMotion.

Opportunistic

Use encrypted vMotion if source and destination hosts support it. Only ESXi hosts of version 6.5 and later use encrypted vMotion.

Required

Allow only encrypted vMotion. If the source or destination host does not support encrypted vMotion, migration with vMotion fails.

Virtual Machine Conditions and Limitations for vMotion

To migrate virtual machines with vMotion, the virtual machine must meet certain network, disk, CPU, USB, and other device requirements.

The following virtual machine conditions and limitations apply when you use vMotion:

- The source and destination management network IP address families must match. You cannot migrate a virtual machine from a host that is registered to vCenter Server with an IPv4 address to a host that is registered with an IPv6 address.

- Using 1 GbE network adapters for the vMotion network might result in migration failure, if you migrate virtual machines with large vGPU profiles. Use 10 GbE network adapters for the vMotion network.

- If virtual CPU performance counters are enabled, you can migrate virtual machines only to hosts that have compatible CPU performance counters.

- You can migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use the graphics renderer that is present on the destination host. The renderer can be the host CPU or a GPU graphics card. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU graphics card.

- Starting with vSphere 6.7 Update 1 and later, vSphere vMotion supports virtual machines with vGPU.

- vSphere DRS supports initial placement of vGPU virtual machines running vSphere 6.7 Update 1 or later without load balancing support.

- You can migrate virtual machines with USB devices that are connected to a physical USB device on the host. You must enable the devices for vMotion.

- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host. For example, you cannot migrate a virtual machine with a CD drive backed by the physical CD drive on the source host. Disconnect these devices before you migrate the virtual machine.

- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer. Disconnect these devices before you migrate the virtual machine.

Using vMotion to Migrate vGPU Virtual Machines

You can use vMotion to perform a live migration of NVIDIA vGPU-powered virtual machines without causing data loss.

In vSphere 6.7 Update 1 and vSphere 6.7 Update 2, when you migrate vGPU virtual machines with vMotion and vMotion stun time exceeds 100 seconds, the migration process might fail for vGPU profiles with 24 GB frame buffer size or larger. To avoid the vMotion timeout, upgrade to vSphere 6.7 Update 3 or later.

During the stun time, you are unable to access the VM, desktop, or application. Once the migration is completed, access to the VM resumes and all applications continue from their previous state. For information on frame buffer size in vGPU profiles, refer to the NVIDIA Virtual GPU documentation.

The expected VM stun times (the time when the VM is inaccessible to users during vMotion) are listed in the following table. These stun times were tested over a 10Gb network with NVIDIA Tesla V100 PCIe 32 GB GPUs :

Table 12-1. Expected Stun Times for vMotion of vGPU VMs

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
1	1.95
2	3.18
4	5.74
8	11.05

Table 12-1. Expected Stun Times for vMotion of vGPU VMs (continued)

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
16	21.32
32	38.83

Note The configured vGPU profile represents an upper bound to the used vGPU frame buffer. In many use cases, the amount of vGPU frame buffer memory used by the VM at any given time is below the assigned vGPU memory in the profile. Treat these times as worst case stun times for cases when the entire assigned vGPU memory is being used at the time of the migration. For example, a V100-32Q vGPU profile allocates 32 GB of vGPU frame buffer to the VM, but the VM can use any amount between 0-32 GB of frame buffer during the migration. As a result, the stun time can end up being between less than 1 second to 38.83 seconds.

DRS supports initial placement of vGPU VMs running vSphere 6.7 Update 1 and later without load balancing support.

VMware vSphere vMotion is supported only with and between compatible NVIDIA GPU device models and NVIDIA GRID host driver versions as defined and supported by NVIDIA. For compatibility information, refer to the NVIDIA Virtual GPU User Guide.

To check compatibility between NVIDIA vGPU host drivers, vSphere, and Horizon, refer to the VMware Compatibility Matrix.

Swap File Location Compatibility

Virtual machine swap file location affects vMotion compatibility in different ways depending on the version of ESXi running on the virtual machine's host.

You can configure ESXi 6.5 or later hosts to store virtual machine swap files with the virtual machine configuration file, or on a local swap file datastore specified for that host.

The location of the virtual machine swap file affects vMotion compatibility as follows:

- For migrations between hosts running ESXi 6.5 and later, vMotion and migrations of suspended and powered-off virtual machines are allowed.

- During a migration with vMotion, if the swap file location on the destination host differs from the swap file location on the source host, the swap file is copied to the new location. This activity can result in slower migrations with vMotion. If the destination host cannot access the specified swap file location, it stores the swap file with the virtual machine configuration file.

See the *vSphere Resource Management* documentation for information about configuring swap file policies.

Migration with vMotion in Environments Without Shared Storage

You can use vMotion to migrate virtual machines to a different compute resource and storage simultaneously. Unlike Storage vMotion, which requires a single host to have access to both the

source and destination datastore, you can migrate virtual machines across storage accessibility boundaries.

vMotion does not require environments with shared storage. This is useful for performing cross-cluster migrations, when the target cluster machines might not have access to the storage of the source cluster. Processes that are working on the virtual machine continue to run during the migration with vMotion.

You can use vMotion to migrate virtual machines across vCenter Server instances.

You can place the virtual machine and all its disks in a single location or select separate locations for the virtual machine configuration file and each virtual disk. In addition, you can change virtual disks from thick-provisioned to thin-provisioned or from thin-provisioned to thick-provisioned. For virtual compatibility mode RDMs, you can migrate the mapping file or convert from RDM to VMDK.

vMotion without shared storage is useful for virtual infrastructure administration tasks similar to vMotion with shared storage or Storage vMotion tasks.

- Host maintenance. You can move virtual machines from a host to allow maintenance of the host.

- Storage maintenance and reconfiguration. You can move virtual machines from a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.

- Storage load redistribution. You can manually redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Requirements and Limitations for vMotion Without Shared Storage

A virtual machine and its host must meet resource and configuration requirements for the virtual machine files and disks to be migrated with vMotion in the absence of shared storage.

vMotion in an environment without shared storage is subject to the following requirements and limitations:

- The hosts must be licensed for vMotion.

- The hosts must be running ESXi 5.1 or later.

- The hosts must meet the networking requirement for vMotion. See vSphere vMotion Networking Requirements.

- The virtual machines must be properly configured for vMotion. See Virtual Machine Conditions and Limitations for vMotion

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). See Storage vMotion Requirements and Limitations.

- The destination host must have access to the destination storage.

- When you move a virtual machine with RDMs and do not convert those RDMs to VMDKs, the destination host must have access to the RDM LUNs.

- Consider the limits for simultaneous migrations when you perform a vMotion migration without shared storage. This type of vMotion counts against the limits for both vMotion and Storage vMotion, so it consumes both a network resource and 16 datastore resources. See Limits on Simultaneous Migrations.

Migration Between vCenter Server Systems

vSphere 6.0 or later lets you migrate virtual machines between vCenter Server instances.

Migration of virtual machines across vCenter Server systems is helpful in certain VM provisioning cases.

- Balance workloads across clusters and vCenter Server instances.

- Elastically expand or shrink capacity across resources in different vCenter Server instances in the same site or in another geographical area .

- Move virtual machines between environments that have different purposes, for example, from a development to production.

- Move virtual machines to meet different Service Level Agreements (SLAs) regarding storage space, performance, and so on.

Note   During the migration of a virtual machine to another vCenter Server system, the performance data that has been collected about the virtual machine is lost.

- Requirements for Migration Between vCenter Server Instances

  You can use migration across vCenter Server instances if your system meets certain requirements.

- Network Compatibility Checks During vMotion Between vCenter Server Instances

  Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

- MAC Address Management During Migration Between vCenter Server Systems

  When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

- Export a Virtual Machine with Advanced Cross vCenter vMotion

  With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

- Import a Virtual Machine with Advanced Cross vCenter vMotion

   With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Requirements for Migration Between vCenter Server Instances

You can use migration across vCenter Server instances if your system meets certain requirements.

The following list sums the requirements that your system must meet so that you can use migration across vCenter Server instances:

- The cross vCenter Server and long-distance vMotion features require an Enterprise Plus license. For more information, see http://www.vmware.com/uk/products/vsphere/compare.html.

- To migrate virtual machines across vCenter Server instances in different vCenter Single Sign-On domains, you can use Advanced Cross vCenter vMotion. The vCenter Server instance from which you initiate the import or export of virtual machines must be version 7.0 Update 1c or later.

- When you migrate virtual machines across vCenter Server instances in Enhanced Linked Mode, without using Advanced Cross vCenter vMotion, verify that you meet the following requirements.

   - The source and destination vCenter Server instances and ESXi hosts must be 6.0 or later.

   - Both vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification.

   - For migration of compute resources only, both vCenter Server instances must be connected to the shared virtual machine storage.

   - Both vCenter Server instances must be in the same vCenter Single Sign-On domain. Enhanced Link Mode lets the source vCenter Server authenticate to the destination vCenter Server

      For information about installing vCenter Server in Enhanced Linked Mode, see the *vCenter Server Installation and Setup* documentation.

Network Compatibility Checks During vMotion Between vCenter Server Instances

Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

vCenter Server performs network compatibility checks to prevent the following configuration problems:

- MAC address compatibility on the destination host

- vMotion from a distributed switch to a standard switch

- vMotion between distributed switches of different versions

- vMotion to an internal network, for example, a network without a physical NIC

- vMotion to a distributed switch that is not working properly

vCenter Server does not perform checks for and notify you about the following problems:

- If the source and destination distributed switches are not in the same broadcast domain, virtual machines lose network connectivity after migration.

- If the source and destination distributed switches do not have the same services configured, virtual machines might lose network connectivity after migration.

MAC Address Management During Migration Between vCenter Server Systems

When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

In an environment with multiple vCenter Server instances, when a virtual machine is migrated, its MAC addresses are transferred to the target vCenter Server. The source vCenter Server adds the MAC addresses to a denylist so that it does not assign them to newly created virtual machines.

To reclaim unused MAC addresses from the denylist, contact VMware Technical Support for assistance.

Export a Virtual Machine with Advanced Cross vCenter vMotion

With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

With Advanced Cross vCenter vMotion, you can migrate virtual machines to a vCenter Server instance in a different vCenter Single Sign-On domain. For example, when you deploy a new vCenter Server instance, you can migrate virtual machines from the earlier version of your vCenter Server instance to the newly provisioned one.

Prerequisites

- Obtain the credentials for the administrator accounts of the vCenter Server instances to which you want to migrate virtual machines.

- Verify that the target vCenter Server instances are version 6.5 or later.

- Verify that the source vCenter Server instance is version 7.0 Update 1c or later.

- If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, verify that the destination host or cluster have available PMem resources.

- If you migrate a virtual machine that has an NVDIMM device or a vPMem disk, verify that the destination host has the proper license.

- Required privilege: **Resource.Query vMotion**

- When you migrate powered on virtual machines, verify that you meet the following requirements.

  - Required privilege: **Resource.Migrate powered on virtual machine**

  - Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See Host Configuration for vMotion and Virtual Machine Conditions and Limitations for vMotion.

  - Verify that your hosts and virtual machines meet the requirements for live migration. See Requirements and Limitations for vMotion Without Shared Storage.

- When you migrate powered off virtual machines, verify that you meet the following requirements.

  - Required privilege: **Resource.Migrate powered off virtual machine**

  - Make sure that you are familiar with the requirements for cold migration. See Cold Migration.

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 From the inventory tree, select the host or cluster that contains the virtual machines you want to migrate.

3 On the **VMs** tab, click the **Virtual Machines** button.

4 From the virtual machines list, select the virtual machines you want to migrate.

5 Right-click the selection and click **Migrate**.

6 If a confirmation dialogue box appears, click **Yes**.

   The migration wizard appears.

7 Select **Cross vCenter Server export** as the migration type, and click **Next**.

8 Select the target vCenter Server instance to which you want to export virtual machines.

Option	Action
Saved vCenters	From the drop-down menu, select a saved vCenter Server IP address or an FQDN.
New vCenter	a Enter the IP address or FQDN, user name, and password of a vCenter Server instance. **Note** The check box **Save vCenter Server address** is selected by default. If you do not want to save the vCenter Server address, deselect the check box. b Click **Login**.

Connection to the saved vCenter Server instances is valid only for the current user session. You must enter the credentials of the target vCenter Server instances in each login session.

9 If a **Security Alert** dialog box appears, click **Yes**.

10 Click **Next**.

11 Select the destination compute resource for this virtual machine migration and click **Next**.

Possible targets include hosts and DRS clusters with any level of automation. If DRS is not enabled for a cluster, select a specific host in the cluster rather than selecting the cluster.

Important   If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important   When you try to migrate a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license, the operation fails and the virtual machine is in an unmanageable state for 90 seconds. After 90 seconds, you can retry the migration, and select a destination host that is licensed to use PMem devices.

12 If a compatibility problem appears in the Compatibility pane, fix the problem or select another host or cluster for the migration.

13 Select the destination storage for the virtual machine migration.

    a   Select the storage type for the virtual machine configuration files and all the hard disks.

Mode	Description
Standard	All virtual disks are stored on a standard datastore.
PMem	All virtual disks are stored on the local PMem datastore of the host. Configuration files cannot be stored on a PMem datastore. You must additionally select a regular datastore for the configuration files of the virtual machine.
Hybrid	All PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and your choice of a datastore or a datastore cluster affects non-PMem disks.

You can select the type of storage only if PMem or Hybrid storage types are available in the data center.

    b   Select the format for the virtual machine disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

c   Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

---

d   Select the datastore location for the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1 Select a Storage DRS cluster. 2 (Optional) If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3 Click **Next**.

Store virtual machine configuration files and disks in separate locations.	1 Click **Configure per disk**.
	    Note You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage.
	2 For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster.
	    Note Configuration files cannot be stored on a PMem datastore.
	3 (Optional) If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster.
	4 Click **Next**.

14 If a compatibility problem appears in the Compatibility pane, fix the problem or select another destination storage for the migration.

15 Select the destination folder for the virtual machine migration and click **Next**.

16 Select the destination networks for the virtual machine migration.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	a Click the arrow in the **Destination Network** column and select **Browse**. b Select a destination network and click **OK**. c Click **Next**.
Select a different destination network for each VM network adapter connected to a valid source network.	a Click **Advanced**. b Click the arrow in the **Destination Network** column and select **Browse**. c Select a destination network and click **OK**. d Click **Next**.

17 On the **Ready to complete** page, review the details and click **Finish**.

Results

The virtual machines are moved to the destination folder in the new vCenter Server instance. You can monitor the migration process in the **Recent tasks** pane. If errors occur during the migration, the virtual machines revert to their original states and locations.

Import a Virtual Machine with Advanced Cross vCenter vMotion

With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

With Advanced Cross vCenter vMotion, you can import virtual machines from a vCenter Server instance in a different vCenter Single Sign-On domain. For example, when you deploy a new vCenter Server instance, you can migrate virtual machines from the earlier version of your vCenter Server instance to the newly provisioned one.

Prerequisites

- Obtain the credentials for the administrator account of the vCenter Server instance from which you want to import virtual machines.

- Verify that the source vCenter Server instances are version 6.5 or later.

- Verify that the target vCenter Server instance is version 7.0 Update 1c or later.

- If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, verify that the destination host or cluster have available PMem resources.

- If you migrate a virtual machine that has an NVDIMM device or a vPMem disk, verify that the destination host has the proper license.

- Required privilege: **Resource.Query vMotion**

- When you migrate powered on virtual machines, verify that you meet the following requirements.

    - Required privilege: **Resource.Migrate powered on virtual machine**

    - Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See Host Configuration for vMotion and Virtual Machine Conditions and Limitations for vMotion.

    - Verify that your hosts and virtual machines meet the requirements for live migration. See Requirements and Limitations for vMotion Without Shared Storage.

- When you migrate powered off virtual machines, verify that you meet the following requirements.

    - Required privilege: **Resource.Migrate powered off virtual machine**

- Make sure that you are familiar with the requirements for cold migration. See Cold Migration.

Procedure

1 In the vSphere Client home page, navigate to **Home > Hosts and Clusters**.

2 From the inventory tree, right-click the host or cluster to which you want to import virtual machines.

3 Click **Import VMs**.

   The migration wizard appears.

4 Select the source vCenter Server instance from which you want to import virtual machines.

Option	Action
Saved vCenters	From the drop-down menu, select a saved vCenter Server IP addressor an FQDN.
New vCenter	a Enter the IP address or FQDN, user name, and password of a vCenter Server instance. **Note** The check box **Save vCenter Server address** is selected by default. If you do not want to save the vCenter Server address, deselect the check box. b Click **Login**.

Connection to the saved vCenter Server instances is valid only for the current user session. You must enter the credentials of the source vCenter Server instances in each login session.

5 If a **Security Alert** dialog box appears, click **Yes**.

6 Click **Next**.

7 Select the virtual machines to import and click **Next**.

   If you want to migrate more than one virtual machine, the selected virtual machines must be in the same power state.

8 Select the destination compute resource for this virtual machine migration and click **Next**.

   Possible targets include hosts and DRS clusters with any level of automation. If DRS is not enabled for a cluster, select a specific host in the cluster rather than selecting the cluster.

   Important If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

   Important When you try to migrate a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license, the operation fails and the virtual machine is in an unmanageable state for 90 seconds. After 90 seconds, you can retry the migration, and select a destination host that is licensed to use PMem devices.

9 If a compatibility problem appears in the Compatibility pane, fix the problem or select another host or cluster for the migration.

10 Select the destination storage for the virtual machine migration.

a Select the storage type for the virtual machine configuration files and all the hard disks.

Mode	Description
Standard	All virtual disks are stored on a standard datastore.
PMem	All virtual disks are stored on the local PMem datastore of the host. Configuration files cannot be stored on a PMem datastore. You must additionally select a regular datastore for the configuration files of the virtual machine.
Hybrid	All PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and your choice of a datastore or a datastore cluster affects non-PMem disks.

You can select the type of storage only if PMem or Hybrid storage types are available in the data center.

b Select the format for the virtual machine disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

c   Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

d   Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1 Select a Storage DRS cluster. 2 (Optional) If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3 Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1 Click **Configure per disk**. **Note** You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage. 2 For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note** Configuration files cannot be stored on a PMem datastore. 3 (Optional) If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4 Click **Next**.

11 If a compatibility problem appears in the Compatibility pane, fix the problem or select another destination storage for the migration.

12 Select the destination folder for the virtual machines and click **Next**.

13 Select the destination networks for the virtual machine migration.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	a Click the arrow in the **Destination Network** column and select **Browse**. b Select a destination network and click **OK**. c Click **Next**.
Select a different destination network for each VM network adapter connected to a valid source network.	a Click **Advanced**. b Click the arrow in the **Destination Network** column and select **Browse**. c Select a destination network and click **OK**. d Click **Next**.

14 On the **Ready to complete** page, review the details and click **Finish**.

Results

The virtual machines are moved to the destination folder in the current vCenter Server instance. You can monitor the migration process in the **Recent tasks** pane. If errors occur during the migration, the virtual machines revert to their original states and locations.

Migration with Storage vMotion

With Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running. With Storage vMotion, you can move virtual machines off of arrays for maintenance or to upgrade. You also have the flexibility to optimize disks for performance, or to transform disk types, which you can use to reclaim space.

You can choose to place the virtual machine and all its disks in a single location, or you can select separate locations for the virtual machine configuration file and each virtual disk. The virtual machine does not change execution host during a migration with Storage vMotion.

During a migration with Storage vMotion, you can change the disk provisioning type.

Migration with Storage vMotion changes virtual machine files on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and `.nvram` files. If the new names exceed the maximum filename length, the migration does not succeed.

Storage vMotion has several uses in administering virtual infrastructure, including the following examples of use.

- Storage maintenance and reconfiguration. You can use Storage vMotion to move virtual machines off a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.

- Redistributing storage load. You can use Storage vMotion to redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Storage vMotion Requirements and Limitations

A virtual machine and its host must meet resource and configuration requirements for the virtual machine disks to be migrated with Storage vMotion.

Storage vMotion is subject to the following requirements and limitations:

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thin-provisioned disks during migration if the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.

- Migration of virtual machines during VMware Tools installation is not supported.

- Because VMFS3 datastores do not support large capacity virtual disks, you cannot move virtual disks greater than 2 TB from a VMFS5 datastore to a VMFS3 datastore.

- The host on which the virtual machine is running must have a license that includes Storage vMotion.

- ESXi 4.0 and later hosts do not require vMotion configuration to perform migration with Storage vMotion.

- The host on which the virtual machine is running must have access to both the source and target datastores.

- For limits on the number of simultaneous migrations with vMotion and Storage vMotion, see Limits on Simultaneous Migrations.

CPU Compatibility and EVC

vCenter Server performs compatibility checks before it allows migration of running or suspended virtual machines to ensure that the virtual machine is compatible with the target host.

vMotion transfers the running state of a virtual machine between underlying ESXi systems. Live migration requires that the processors of the target host provide the same instructions to the virtual machine after migration that the processors of the source host provided before migration. Clock speed, cache size, and number of cores can differ between source and target processors. However, the processors must come from the same vendor class (AMD or Intel) to be vMotion compatible.

Note Do not add virtual ESXi hosts to an EVC cluster. ESXi virtual machines are not supported in Enhanced vMotion Compatibility (EVC) clusters.

Migrations of suspended virtual machines also require that the virtual machine be able to resume execution on the target host using equivalent instructions.

When you initiate a migration with vMotion or a migration of a suspended virtual machine, the **Migrate Virtual Machine** wizard checks the destination host for compatibility. If compatibility problems prevent migration, the wizard displays an error message.

The CPU instruction set available to the operating system and to applications running in a virtual machine is determined at the time that a virtual machine is powered on. This CPU feature set is based on the following items:

- Host CPU family and model

- Settings in the BIOS that might disable CPU features

- ESXi version running on the host

- The compatibility setting of the virtual machine

- The guest operating system of the virtual machine

To improve CPU compatibility between hosts of varying CPU feature sets, some host CPU features can be hidden from the virtual machine by placing the host in an Enhanced vMotion Compatibility (EVC) cluster. For more information about EVC, see About Enhanced vMotion Compatibility.

Note You can hide Host CPU features from a virtual machine by applying a custom CPU compatibility mask to the virtual machine, but this is not recommended. VMware, in partnership with CPU and hardware vendors, is working to maintain vMotion compatibility across the widest range of processors. For additional information, search the VMware Knowledge Base for the *vMotion and CPU Compatibility FAQ*.

CPU Compatibility Scenarios

vCenter Server's CPU compatibility checks compare the CPU features available on the source host, the subset of features that the virtual machine can access, and the features available on the target host. Without the use of EVC, any mismatch between user-level features of the hosts blocks migration, whether or not the virtual machine itself has access to those features. A mismatch between kernel-level features of the hosts blocks migration only when the virtual machine has access to a feature that the target host does not provide.

User-level features are non-privileged instructions used by virtual machine applications. These include SSE3, SSSE3, SSE4.1, SSE4.2, and AES. Because they are user-level instructions that bypass the virtualization layer, these instructions can cause application instability if mismatched after a migration with vMotion.

Kernel-level features are privileged instructions used by the virtual machine operating system. These include the AMD No eXecute (NX) and the Intel eXecute Disable (XD) security features.

When you attempt to migrate a virtual machine with vMotion, one of the following scenarios applies:

- The destination host feature set matches the CPU feature set of the virtual machine. CPU compatibility requirements are met, and migration with vMotion proceeds.

- The CPU feature set of the virtual machine contains features not supported by the destination host. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.

  Note EVC overcomes such incompatibility by providing a "baseline" feature set for all virtual machines running in a cluster. This baseline feature set hides the differences among the clustered hosts' CPUs from the virtual machines.

- The destination host supports the feature set of the virtual machine, plus additional user-level features (such as SSE4.1) not found in the feature set of the virtual machine. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.

  Note This type of incompatibility is ignored for migrations among hosts in EVC clusters.

- The destination host supports the feature set of the virtual machine, plus additional kernel-level features (such as NX or XD) not found in the feature set of the virtual machine. CPU compatibility requirements are met, and migration with vMotion proceeds. The virtual machine retains its CPU feature set while it remains powered on, allowing it to migrate freely back to the original host. However, if the virtual machine is rebooted, it acquires a new feature set from the new host. This process might cause vMotion incompatibility if you attempt to migrate the virtual machine back to the original host.

CPU Families and Feature Sets

Processors are grouped into families. Processors within a given family generally have similar feature sets.

Processor vendors define processor families. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features. Sometimes, processor vendors have introduced significant architectural changes within the same processor family, such as the SSSE3 and SSE4.1 instructions, and NX/XD CPU security features.

By default, vCenter Server identifies mismatches on features accessible to applications as incompatible to guarantee the stability of virtual machines after migrations with vMotion.

Server hardware's CPU specifications usually indicate whether or not the CPUs contain the features that affect vMotion compatibility.

For more information on identifying Intel processors and their features, see *Application Note 485: Intel® Processor Identification and the CPUID Instruction*, available from Intel. For more information on identifying AMD processors and their features, see *CPUID Specification*, available from AMD.

About Enhanced vMotion Compatibility

You can use the Enhanced vMotion Compatibility (EVC) feature to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs.

Configure EVC from the cluster settings dialog box. When you configure EVC, you configure all host processors in the cluster to present the feature set of a baseline processor. This baseline feature set is called the EVC mode. EVC uses AMD-V Extended Migration technology (for AMD hosts) and Intel FlexMigration technology (for Intel hosts) to mask processor features so that hosts can present the feature set of an earlier generation of processors. The EVC mode must be equivalent to, or a subset of, the feature set of the host with the smallest feature set in the cluster.

EVC masks only those processor features that affect vMotion compatibility. Enabling EVC does not prevent a virtual machine from taking advantage of faster processor speeds, increased numbers of CPU cores, or hardware virtualization support that might be available on newer hosts.

EVC cannot prevent virtual machines from accessing hidden CPU features in all circumstances. Applications that do not follow CPU vendor recommended methods of feature detection might behave unexpectedly in an EVC environment. VMware EVC cannot be supported with ill-behaved applications that do not follow the CPU vendor recommendations. For more information about creating well-behaved applications, search the VMware Knowledge Base for the article *Detecting and Using New Features in CPUs*.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

EVC Requirements for Hosts

To improve CPU compatibility between hosts that have varying CPU feature sets, you can hide some host CPU features from the virtual machines by placing the host in an Enhanced vMotion Compatibility (EVC) cluster. Hosts in an EVC cluster and hosts that you add to an existing EVC cluster must meet EVC requirements.

- Power off all virtual machines in the cluster that are running on hosts with a feature set greater than the EVC mode that you intend to enable. You can also migrate these virtual machines out of the cluster.

- All hosts in the cluster must meet the following requirements:

Requirements	Description
Supported ESXi version	ESXi 6.5 or later.
vCenter Server	The host must be connected to a vCenter Server system.
CPUs	A single vendor, either AMD or Intel.
Advanced CPU features enabled	Enable these CPU features in the BIOS if they are available: ■ Hardware virtualization support (AMD-V or Intel VT) ■ AMD No eXecute(NX) ■ Intel eXecute Disable (XD) **Note** Hardware vendors sometimes disable particular CPU features in the BIOS by default. You might have problems enabling EVC because the EVC compatibility checks detect the absence of features that are expected to be present for a particular CPU. If you cannot enable EVC on a system with a compatible processor, ensure that all features are enabled in the BIOS.
Supported CPUs for the EVC mode that you want to enable	To check EVC support for a specific processor or server model, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.
Configured for vMotion	See Host Configuration for vMotion.

Enable EVC on an Existing Cluster

Enable EVC on an existing cluster to ensure vMotion CPU compatibility between the hosts in the cluster. Other cluster features such as vSphere DRS and vSphere HA are fully compatible with EVC.

Prerequisites

Verify that the hosts in the cluster meet the requirements listed in EVC Requirements for Hosts.

Procedure

1 Select a cluster in the vSphere inventory.

2 Power off all the virtual machines on the hosts with feature sets greater than the EVC mode.

3 Click the **Configure** tab, select VMware EVC, and click **Edit**.

4 Enable EVC for the CPU vendor and feature set appropriate for the hosts in the cluster, and click **OK**.

5 Power on the virtual machines in the cluster to apply the EVC.

Change the EVC Mode for a Cluster

Configure EVC to ensure that virtual machine migrations between hosts in the cluster do not fail because of CPU feature incompatibilities.

Several EVC approaches are available to ensure CPU compatibility:

■ If all the hosts in a cluster are compatible with a newer EVC CPU or Graphics (vSGA) mode, you can change the EVC CPU or Graphics (vSGA) mode of an existing EVC cluster.

■ You can enable EVC for a cluster that does not have EVC enabled.

■ You can raise the EVC mode to expose more CPU features.

■ You can lower the EVC mode to hide CPU features and increase compatibility.

Prerequisites

■ Verify that all hosts in the cluster have supported CPUs for the EVC mode you want to enable. See Knowledge Base article KB 1003212 for a list of supported CPUs.

■ Verify that all hosts in the cluster are connected and registered on vCenter Server. The cluster cannot contain a disconnected host.

■ Virtual machines must be in the following power states, depending on whether you raise or lower the EVC mode.

EVC Mode	Virtual Machine Power Action
Raise the EVC mode to a CPU baseline with more features.	Running virtual machines can remain powered on. New EVC mode features are not available to the virtual machines until they are powered off and powered back on again. A full power cycling is required. Rebooting the guest operating system or suspending and resuming the virtual machine is not sufficient.
Lower the EVC mode to a CPU baseline with fewer features.	Power off virtual machines if they are powered on and running at a higher EVC Mode than the one you intend to enable.

To verify the EVC mode for virtual machines, see Determine the EVC Mode of a Virtual Machine.

Procedure

1   Select a cluster in the inventory.

2   Click the **Configure** tab.

3   Under **Configuration**, select **VMware EVC**, and click **Edit**.

4   On the **Change EVC Mode** page, select whether to enable or disable EVC.

Option	Description
Disable EVC	The EVC feature is disabled. CPU compatibility is not enforced for the hosts in this cluster.
Enable EVC for AMD Hosts	The EVC feature is enabled for AMD hosts.
Enable EVC for Intel Hosts	The EVC feature is enabled for Intel hosts.

5   From the **CPU Mode** drop-down menu, select the baseline CPU feature set that you want to enable for the cluster.

    If you cannot select the EVC CPU Mode, the Compatibility pane displays the reason, and the relevant hosts for each reason.

6   (Optional) From the **Graphics Mode (vSGA)** drop-down menu, select a baseline graphics feature set.

    If you cannot select the EVC vSGA Mode, the Compatibility pane displays the reason, and the relevant hosts for each reason.

Option	Description
Baseline Graphics	Applies the Baseline Graphics feature set that includes features through Direct3D 10.1/OpenGL 3.3.
	Note **Graphics Mode (vSGA)** applies only the Baseline Graphics set that includes features through Direct3D 10.1/OpenGL 3.3. The Baseline Graphics feature set is compatible with all supported features for ESXi 7.0 or earlier.
D3D 11.0 class features	Applies the baseline graphics feature set that includes features through Direct3D 11.0/OpenGL 4.1.
	Note When you create a cluster, if you enable EVC graphics mode D3D 11.0 class features, you can add only ESXi hosts that support Direct3D 11.0 to the cluster. When you try to add an ESXi host that does not support Direct3D 11.0 to the cluster, the operation fails with an error message.

7   Click **OK**.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU and graphics features that a host must have in order for the virtual machine to migrate to that host and power on. The EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine powers on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it runs. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, you create an EVC cluster that contains hosts with Intel processors and you set the EVC mode to Intel "Merom" Generation (Xeon Core 2). When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If you raise the EVC mode of the cluster to Intel "Penryn" Generation (Xeon 45 nm Core 2), the virtual machine retains the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use the feature set of the higher EVC mode, such as SSE4.1, the virtual machine must be powered off and powered on again.

Procedure

1 Navigate to a cluster or a host in the vCenter Server inventory.

2 Click the **VMs** tab.

   A list of all virtual machines in the selected cluster or on the selected host appears.

3 To verify the status of the CPU mode, check the **EVC CPU Mode** column.

   a Click the angle icon next to any column title and select **Show/Hide Columns > EVC CPU Mode**.

The **EVC CPU Mode** column shows the CPU modes of all virtual machines in the cluster or on the host.

Important For each virtual machine, the **EVC CPU Mode** column displays the EVC mode defined at the virtual machine level.

However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the **EVC CPU Mode** column displays the inherited EVC mode of the parent host or cluster.

If the virtual machine is in an EVC cluster, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

- When the virtual machine is powered on, the **EVC CPU Mode** column displays either the per-VM EVC mode, or the cluster-level EVC mode.

Per-VM EVC	Cluster-Level EVC	EVC Mode for the Virtual Machine
Enabled	Enabled	Enabled. The **EVC CPU Mode** column displays the EVC mode of the virtual machine.
Disabled	Enabled	Enabled. The **EVC CPU Mode** column displays the EVC mode of the EVC cluster.

- When the virtual machine is powered off, the **EVC CPU Mode** column displays the per-VM EVC mode. If per-VM EVC is disabled, the **EVC CPU Mode** column for the virtual machine is empty.

When the virtual machine is not in an EVC cluster and per-VM EVC is not configured, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

- When the virtual machine is powered on, the **EVC CPU Mode** column displays the EVC mode of the parent host.

- When the virtual machine is powered off, the **EVC CPU Mode** column is empty.

4 To verify the status of the graphics mode, check the **EVC Graphics Mode (vSGA)** column.

  a Click the angle icon next to any column title and select **Show/Hide Columns > EVC Graphics Mode (vSGA)**.

The **EVC Graphics Mode (vSGA)** column displays the baseline graphics features set. To view the baseline graphics, you must enable **3D graphics** in the virtual machine.

For information about configuring 3D graphics in a virtual machine, see the *vSphere Virtual Machine Administration* guide.

Determine the EVC Mode that a Host Supports

By determining the EVC modes that the host can support, you can determine whether the host is compatible with other hosts in an EVC cluster. For hosts to be included in the same EVC cluster, all the hosts must support at least one common mode.

Procedure

1   Select a host in the inventory.

2   Click the **Summary** tab.

3   In the Configuration panel, expand **EVC Mode**.

The supported EVC modes are listed in order from the fewest to the greatest number of supported features.

Prepare Clusters for AMD Processors Without 3DNow!

Newer generations of AMD processors do not include 3DNow! processor instructions. If hosts in a cluster have different generations of AMD processors, some with 3DNow! instruction sets and some without, you cannot successfully migrate virtual machines between the hosts. You must use an EVC mode or CPU compatibility mask to hide the instructions.

The vCenter Server **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode masks the 3DNow! instructions from virtual machines. You can apply this EVC mode to EVC clusters containing only AMD Opteron Generation 3 hosts. Applying this mode allows the clusters to maintain vMotion compatibility with AMD Opteron hosts that do not have 3DNow! instructions. Clusters containing AMD Opteron Generation 1 or AMD Opteron Generation 2 hosts cannot be made vMotion-compatible with hosts that do not have 3DNow! instructions.

Prerequisites

Ensure that the cluster contains only hosts with AMD Opteron Generation 3 or newer processors.

Procedure

◆ Enable the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode for your EVC cluster.

The steps to enable the EVC mode differ depending on whether you are creating a cluster or enabling the mode on an existing cluster, and on whether the existing cluster contains powered-on virtual machines.

Option	Description
Creating a cluster	In the New Cluster wizard, enable EVC for AMD hosts and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster without powered-on virtual machines	In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster with powered-on virtual machines	The **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode cannot be enabled while there are powered-on virtual machines in the cluster. a Power-off any running virtual machines in the cluster, or migrate them out of the cluster using vMotion. Migrating the virtual machines out of the cluster with vMotion allows you to delay powering off the virtual machines until a more convenient time. b In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode. c If you migrated virtual machines out of the cluster, power them off and cold migrate them back into the cluster. d Power on the virtual machines.

Results

You can now add hosts with AMD processors without 3DNow! instructions to the cluster and preserve vMotion compatibility between the new hosts and the existing hosts in the cluster.

CPU Compatibility Masks

CPU compatibility masks allow customization of the CPU features visible to a virtual machine.

vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether or not to allow migrations with vMotion.

To guarantee the stability of virtual machines after a migration with vMotion, VMware sets the default values for CPU compatibility masks.

When a choice between CPU compatibility or guest operating system features (such as NX/XD) exists, VMware provides check-box options to configure individual virtual machines. You can access the configuration options through the Advanced Settings option for the CPU of the virtual machine. For more control over the visibility of CPU features, you can edit the CPU compatibility mask of the virtual machine at the bit level.

Caution Changing the CPU compatibility masks can result in an unsupported configuration. Do not manually change the CPU compatibility masks unless instructed to do so by VMware Support or a VMware Knowledge base article.

CPU compatibility masks cannot prevent virtual machines from accessing masked CPU features in all circumstances. In some circumstances, applications can detect and use masked features even though they are hidden from the guest operating system. In addition, on any host, applications that use unsupported methods of detecting CPU features rather than using the CPUID instruction can access masked features. Virtual machines running applications that use unsupported CPU detection methods might experience stability problems after migration.

View CPUID Details for an EVC Cluster

The feature set that is exposed by an EVC cluster corresponds to the feature set of a particular type of processor. Processor feature sets are described by a set of feature flags that you examine using the CPUID instruction.

You can view the CPUID feature flags currently exposed by the hosts in an EVC cluster.

Procedure

1 Select a cluster in the inventory.

2 Click the **Configure** tab.

3 Select **VMware EVC** and expand **Current CPUID Details**.

Results

This VMware EVC panel displays the CPUID feature flags that EVC enforces for the hosts in this cluster. For information about CPUID feature flags, see the Intel and AMD websites.

Migrate a Powered Off or Suspended Virtual Machine

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

Prerequisites

- Make sure that you are familiar with the requirements for cold migration. See Cold Migration.

- Required privilege: **Resource.Migrate powered off virtual machine**

Procedure

1 Power off or suspend the virtual machine.

2 Right-click the virtual machine and select **Migrate**.

    a   To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

    b   Click the **Virtual Machines** tab.

3 Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.

4 If you change the compute resource of the virtual machine, select the destination compute resource for this virtual machine migration and click **Next**.

Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster.

Important If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

5 If you change the storage of the virtual machine, enter the required details in the **Select Storage** page.

a Select the storage type for the virtual machine configuration files and all the hard disks.

- If you select the **Standard** mode, all virtual disks are stored on a standard datastore.

- If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.

- If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

Selecting the type of storage is possible only if PMem or Hybrid storage types are available in the data center.

b Select the format for the virtual machine disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

c   Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important   If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

---

d   Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1 Select a Storage DRS cluster. 2 (Optional) To disable Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3 Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1 Click **Configure per disk**. **Note** You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage. 2 For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note** Configuration files cannot be stored on a PMem datastore. 3 (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4 Click **Next**.

6   If you change the compute resource of the virtual machine, select destination networks for the virtual machine migration.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	a Click the arrow in the **Destination Network** column and select **Browse**. b Select a destination network and click **OK**. c Click **Next**.
Select a new destination network for each VM network adapter connected to a valid source network.	a Click **Advanced**. b Click the arrow in the **Destination Network** column and select **Browse**. c Select a destination network and click **OK**. d Click **Next**.

7   On the **Ready to complete** page, review the details and click **Finish**.

Results

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource

You can use the **Migration** wizard to migrate a powered-on virtual machine from one compute resource to another by using vMotion. To relocate only the disks of a powered-on virtual machine, migrate the virtual machine to a new datastore by using Storage vMotion.

Prerequisites

Verify that your hosts and virtual machines meet the requirements for migration with vMotion with shared storage.

- Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See Host Configuration for vMotion and Virtual Machine Conditions and Limitations for vMotion.

- Verify that the storage that contains the virtual machine disks is shared between the source and target hosts. See vMotion Shared Storage Requirements.

- For migration across vCenter Server instances, verify whether your system meets additional requirements. See Requirements for Migration Between vCenter Server Instances

- For migration of a virtual machine with NVIDIA vGPU, verify that the target ESXi host has a free vGPU slot. Also, verify that the `vgpu.hotmigrate.enabled` advanced setting is set to `true`. For more information about configuring vCenter Server advanced settings, see "Configure Advanced Settings" in *vCenter Server Configuration*.

- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

1 Right-click the virtual machine and select **Migrate**.

   a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

   b Click the **Virtual Machines** tab.

2 Click **Change compute resource only** and click **Next**.

3 Select a host, cluster, resource pool, or vApp to run the virtual machine, and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and fully automated DRS clusters in the same or another vCenter Server system. If your target is a non-automated cluster, select a host within the non-automated cluster.

Important If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

4   Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

5   Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

6   Review the page and click **Finish**.

Results

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource and Storage

You can move a virtual machine to another compute resource and move its disks or virtual machine folder to another datastore. With vMotion, you can migrate a virtual machine and its disks and files while the virtual machine is powered on.

Simultaneous migration to a new compute resource and datastore provides greater mobility for virtual machines by eliminating the vCenter Server boundary. Virtual machine disks or contents of the virtual machine folder are transferred over the vMotion network to reach the destination host and datastores.

To make disk format changes and preserve them, you must select a different datastore for the virtual machine files and disks. You cannot preserve disk format changes if you select the same datastore on which the virtual machine currently resides.

Prerequisites

- Verify that your hosts and virtual machines meet the requirements for live migration. See Requirements and Limitations for vMotion Without Shared Storage.

- For migration across vCenter Server instances, verify whether your system meets additional requirements. See Requirements for Migration Between vCenter Server Instances

- For migration of a virtual machine with NVIDIA vGPU, verify that the target ESXi host has a free vGPU slot. Also, verify that the `vgpu.hotmigrate.enabled` advanced setting is set to `true`. For more information about configuring vCenter Server advanced settings, see "Configure Advanced Settings" in *vCenter Server Configuration*.

- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

1 Right-click the virtual machine and select **Migrate**.

   a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

   b Click the **Virtual Machines** tab.

2 Select **Change both compute resource and storage** and click **Next**.

3 Select a destination resource for the virtual machine, and click **Next**.

Any compatibility problems appear in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and fully automated DRS clusters. If your target is a non-automated cluster, select a host within the non-automated cluster.

If your environment has more than one vCenter Server instances, you can move virtual machines from one vCenter Server inventory to another.

Important If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

4   Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

5   Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

6 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. c Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. **Note** You can use the **Advanced** option to downgrade from or upgrade to PMem storage. b For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note** Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. d Click **Next**.

7 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

8 Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

9 On the Ready to complete page, review the details and click **Finish**.

Results

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to New Storage

Use migration with Storage vMotion to relocate the configuration file of a virtual machine and its virtual disks while the virtual machine is powered on.

You can change the virtual machine host during a migration with Storage vMotion.

Prerequisites

- Verify that your system satisfies the requirements for Storage vMotion. See Storage vMotion Requirements and Limitations.

- For migration of a virtual machine with NVIDIA vGPU, verify that the ESXi host on which the virtual machine runs has a free vGPU slot. Also, verify that the `vgpu.hotmigrate.enabled` advanced setting is set to `true`. For more information about configuring vCenter Server advanced settings, see "Configure Advanced Settings" in *vCenter Server Configuration*.

- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

1 Right-click the virtual machine and select **Migrate**.

   a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

   b Click the **Virtual Machines** tab.

2 Click **Change storage only** and click **Next**.

3 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

4 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

5 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. c Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. **Note** You can use the **Advanced** option to downgrade from or upgrade to PMem storage. b For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note** Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. d Click **Next**.

6 On the Ready to complete page, review the details and click **Finish**.

Results

vCenter Server moves the virtual machine to the new storage location. Names of migrated virtual machine files on the destination datastore match the inventory name of the virtual machine.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host

Use the vMotion TCP/IP stack to isolate traffic for vMotion and to assign a dedicated default gateway, routing table, and DNS configuration for this traffic. To enable the vMotion TCP/IP stack, assign a new VMkernel adapter to it.

By using a separate TCP/IP stack, you can handle vMotion and cold migration traffic according to the topology of the network and as required for your organization:

- Route the traffic for migration of powered on or powered off virtual machines by using a default gateway. The gateway must be different from the gateway assigned to the default stack on the host.

  By using a separate default gateway, you can use DHCP for IP address assignment to the VMkernel adapters for migration in a flexible way.

- Assign a separate set of buffers and sockets.

- Avoid routing table conflicts that might otherwise appear when many features are using a common TCP/IP stack.

- Isolate traffic to improve security.

Prerequisites

Verify that the host is running ESXi 6.0 or later

Procedure

1 In the vSphere Client, navigate to the host.

2 Click the **Configure** tab.

3 Select **Networking**, and click **VMkernel adapters**.

4 Click **Add networking**.

5 On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.

6 On the Select target device page, select the switch for the VMkernel adapter, and click **Next**.

Option	Description
Select an existing network	Use the physical adapter configuration of an existing distributed port group to send data from the VMkernel adapter to the external network.
Select an existing standard switch	Use the physical adapter configuration for the VMkernel adapter of an existing standard switch.
New vSphere standard switch	Assign a new physical adapter configuration for the VMkernel adapter on a new standard switch.

7 On the Port properties page, select **vMotion** from the **TCP/IP stack** drop-down menu.

The vMotion traffic becomes the only service that is enabled. You cannot use this VMkernel adapter for traffic types other than vMotion.

8 Set the label, VLAN ID, and IP mode of the VMkernel adapter, and click **Next**.

9 (Optional) On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter.
	The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.
	Select the **Override default gateway for this adapter** check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter.

10 (Optional) On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisement to obtain IPv6 addresses.
	In ESXi 6.5 and later router advertisement is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	a Click **Add IPv6 address** to add a new IPv6 address.
	b Enter the IPv6 address and subnet prefix length, and click **OK**.
	c To change the VMkernel default gateway, click **Override default gateway for this adapter**.
	The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

11 Review your settings selections on the Ready to complete page and click **Finish**.

Results

After you create a VMkernel adapter on the vMotion TCP/IP stack, you can use only this stack for vMotion on this host. The VMkernel adapters on the default TCP/IP stack are disabled for the vMotion service. If a live migration uses the default TCP/IP stack while you are configuring VMkernel adapters with the vMotion TCP/IP stack, the migration completes successfully. However, the involved VMkernel adapters on the default TCP/IP stack are disabled for future vMotion sessions.

What to do next

Assign a default gateway, and configure the DNS settings, congestion control, and maximum number of connections for the vMotion TCP/IP stack.

For more information on how to change the configuration of a TCP/IP stack on a host, see the *vSphere Networking* documentation.

Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack

Use the provisioning TCP/IP stack to isolate traffic for cold migration, VM clones, and snapshots, and to assign a dedicated default gateway, routing table, and DNS configuration for this traffic. To enable the Provisioning TCP/IP stack, assign it a new VMkernel adapter.

By using a separate TCP/IP stack, you can handle vMotion and cold migration traffic according to the topology of the network and as required for your organization:

- Route the traffic for migration of powered on or powered off virtual machines by using a default gateway. The gateway must be different from the gateway assigned to the default stack on the host.

  By using a separate default gateway, you can use DHCP for IP address assignment to the VMkernel adapters for migration in a flexible way.

- Assign a separate set of buffers and sockets.

- Avoid routing table conflicts that might otherwise appear when many features are using a common TCP/IP stack.

- Isolate traffic to improve security.

Prerequisites

Verify that the host is running ESXi 6.0 or later

Procedure

1   In the vSphere Client, navigate to the host.

2   Click the **Configure** tab.

3   Select **Networking**, and click **VMkernel adapters**.

4   Click **Add networking**.

5   On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.

6   On the Select target device page, select the switch for the VMkernel adapter, and click **Next**.

Option	Description
Select an existing network	Use the physical adapter configuration of an existing distributed port group to send data from the VMkernel adapter to the external network.
Select an existing standard switch	Use the physical adapter configuration for the VMkernel adapter of an existing standard switch.
New vSphere standard switch	Assign a new physical adapter configuration for the VMkernel adapter on a new standard switch.

7 On the Port properties page, select **Provisioning** from the **TCP/IP stack** drop-down menu.

The provisioning traffic becomes the only service that is enabled. You cannot use this VMkernel adapter for traffic types other than provisioning.

8 Set the label, VLAN ID, and IP mode of the VMkernel adapter, and click **Next**.

9 (Optional) On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter.
	The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.
	Select the **Override default gateway for this adapter** check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter.

10 (Optional) On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisement to obtain IPv6 addresses.
	In ESXi 6.5 and later router advertisement is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	a Click **Add IPv6 address** to add a new IPv6 address.
	b Enter the IPv6 address and subnet prefix length, and click **OK**.
	c To change the VMkernel default gateway, click **Override default gateway for this adapter**.
	The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

11 Review your settings selections on the Ready to complete page and click **Finish**.

Results

After you create a VMkernel adapter on the provisioning TCP/IP stack, you can use only this stack for cold migration, cloning, and snapshots on this host. The VMkernel adapters on the default TCP/IP stack are disabled for the provisioning service. If a live migration uses the default TCP/IP stack while you configure VMkernel adapters with the provisioning TCP/IP stack, the data transfer completes successfully. However, the involved VMkernel adapters on the default TCP/IP stack are disabled for future cold migration, cross-host cloning, and snapshot sessions.

Limits on Simultaneous Migrations

vCenter Server places limits on the number of simultaneous virtual machine migration and provisioning operations that can occur on each host, network, and datastore.

Each operation, such as a migration with vMotion or cloning a virtual machine, is assigned a resource cost. Each host, datastore, or network resource, has a maximum cost that it can support at any one time. Any new migration or provisioning operation that causes a resource to exceed its maximum cost does not proceed immediately, but is queued until other operations complete and release resources. Each of the network, datastore, and host limits must be satisfied for the operation to proceed.

vMotion without shared storage, migrating virtual machines to a different host and datastore simultaneously, is a combination of vMotion and Storage vMotion. This migration inherits the network, host, and datastore costs associated with those operations. vMotion without shared storage is equivalent to a Storage vMotion with a network cost of 1.

Network Limits

Network limits apply only to migrations with vMotion. Network limits depend on the version of ESXi and the network type. All migrations with vMotion have a network resource cost of 1.

Table 12-2. Network Limits for Migration with vMotion

Operation	ESXi Version	Network Type	Maximum Cost
vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	1GigE	4
vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	10GigE	8

Datastore Limits

Datastore limits apply to migrations with vMotion and with Storage vMotion. A migration with vMotion has a resource cost of 1 against the shared virtual machine's datastore. A migration with Storage vMotion has a resource cost of 16 against the source datastore and 16 against the destination datastore.

Table 12-3. Datastore Limits and Resource Costs for vMotion and Storage vMotion

Operation	ESXi Version	Maximum Cost Per Datastore	Datastore Resource Cost
vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	128	1
Storage vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	128	16

Host Limits

Host limits apply to migrations with vMotion, Storage vMotion, and other provisioning operations such as cloning, deployment, and cold migration. All hosts have a maximum cost per host of 8. For example, on an ESXi 5.0 host, you can perform 2 Storage vMotion operations, or 1 Storage vMotion and 4 vMotion operations.

Table 12-4. Host Migration Limits and Resource Costs for vMotion, Storage vMotion, and Provisioning Operations

Operation	ESXi Version	Derived Limit Per Host	Host Resource Cost
vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	8	1
Storage vMotion	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	2	4
vMotion Without Shared Storage	5.1, 5.5, 6.0, 6.5, 6.7, 7.0	2	4
Other provisioning operations	5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	8	1

About Migration Compatibility Checks

During migration, the **Migrate Virtual Machine** wizard checks the destination host for compatibility with the migrating virtual machine using various criteria.

When you select a host or a cluster, the Compatibility panel at the bottom of the **Migrate Virtual Machine** wizard displays information about the compatibility of the selected host or cluster with the virtual machine's configuration.

Compatibility Check Results

If the virtual machine is compatible, the panel displays the message `Compatibility checks succeeded`. If the virtual machine is not compatible with either the host's or cluster's configured networks or datastores, the compatibility window might display both warnings and errors:

- Warning messages do not disable migration. Often the migration is justified and you can continue with the migration despite the warnings.

- Errors might disable migration if no error-free destination hosts are available among the selected destination hosts. In this case, if you click **Next**, the wizard displays the compatibility errors again, and you cannot proceed to the next step.

Compatibility Checks During Migration Setup

When you attempt to move only the compute resource, the **Migrate Virtual Machine** wizard examines the source and destination hosts, the target resource pool, the datastore, and the network. When you attempt to move only the storage, the wizard checks the compatibility of the same objects except for the network.

When you move compute resources and storage together, the **Migrate Virtual Machine** wizard runs fewer compatibility checks. For example, if you move the compute resource, you select the target host or cluster under a vCenter Server instance. The wizard performs all necessary validation only against the selected host, and does not check the datastores available on the destination host. When you attempt to move the virtual machine to a cluster, the **Migrate Virtual Machine** wizard examines the compatibility against the host recommendation from vSphere DRS. The wizard directly validates the compatibility of the target datastore when you select it later.

Another compatibility check is whether vMotion is enabled on the source and target hosts.

Compatibility Checks for Virtual Hardware

Effects of a specific host CPU feature on compatibility depend on whether ESXi exposes or hides them from virtual machines.

- Features that are exposed to virtual machines are not compatible when they do not match on the source and target hosts.

- Features that are not exposed to virtual machines are considered as compatible regardless of whether they match on the hosts.

Specific items of virtual machine hardware can also cause compatibility problems. For example, a virtual machine using an Enhanced VMXNET virtual NIC cannot be migrated to a host running a version of ESXi that does not support Enhanced VMXNET.

Working with the Developer Center

<div style="text-align: right">13</div>

The Developer Center is a single point of entry for developers that provides tools to manage API structure and to capture user actions to translate them into executable code.

This chapter includes the following topics:

- Using the API Explorer

- Using Code Capture

Using the API Explorer

The API Explorer allows you to browse and invoke vSphere REST APIs supported by the system and provides information and context around the API calls.

With the API Explorer, you can choose an API endpoint from your environment and retrieve a list of vSphere REST APIs. You can review details like available parameters, expected responses, and response status codes, and you can invoke the APIs against the live environment. The available APIs depend on the role of the selected endpoint.

Retrieve APIs Using API Explorer

API Explorer retrieves available vSphere REST APIs from a selected endpoint to give you information and context around API calls.

Procedure

1 On the vSphere Client home page, click **Developer Center** and select the **API Explorer** tab.

2 From the **Select Endpoint** drop-down menu, select an endpoint from the environment.

3 From the **Select API** drop-down menu, select an API. The listed APIs are the ones publicly provided by the API explorer in vCenter Server.

4 (Optional) You can use the filter text box to filter your results. For example, enter `health` to view a list of methods related to monitoring the health of the selected API.

5 Select an API category from the list.

6   Select a method from the list.

You can review deprecated APIs by using the toggle button next to each method from the list. Avoid using deprecated APIs. Deprecated APIs might become unresponsive in the future and cause unexpected failures in your automation scripts.

Detailed information about the method appears.

7   If a section about parameter details appears for the selected method, enter a method parameter value in the **Value** text box.

8   (Optional) To invoke the method against the live environment, click **Execute**.

   a   If a warning dialog box appears, click **Yes**.

The result for the invoked method appears in the response box.

9   (Optional) To copy the result for the invoked method to your clipboard, click **Copy Response**.

10 (Optional) To download the result for the invoked method, click **Download**.

Using Code Capture

Code Capture records user actions and translates them into executable code.

Record Actions Using Code Capture

Note   Calls made on operations regarding roles, privileges, tags, content libraries, and storage policies are not recorded. Sensitive data such as passwords is not recorded.

Prerequisites

To use Code Capture to record a session, you must first enable Code Capture.

Procedure

1   From the home sidebar menu, click **Developer Center** and go to the **Code Capture** tab.

2   (Optional) If Code Capture is not enabled, click the toggle to enable Code Capture.

3   To start a recording, navigate to your desired pane and click the red record button in the top pane. To start recording immediately, click **Start Recording**.

While a recording is in progress, the red record button in the top pane blinks.

4   (Optional) To clear the code captured in a previous session and start a new session, click **Clear and Start Another**.

5   To stop a recording, click the red record button in the top pane, or navigate to the **Code Capture** tab in the Developer Center and click **Stop Recording**.

The recorded code appears in the code pane.

6   (Optional) Click **Copy** to copy the code or **Download** to download it as a PowerCLI script.

7 To clear the current code and start another recording, click **Clear and Start Another** or navigate to your desired pane and click the red record button in the top pane.

Results

The recorded code appears in the code pane. You can copy the code, download it, or clear the code to start another recording.

Automating Management Tasks Using vRealize Orchestrator

VMware™ vRealize Orchestrator is a platform that provides a library of extensible workflows. By using the workflow library, you can automate and configure processes to manage the vSphere infrastructure, other VMware technologies, and third-party technologies.

vRealize Orchestrator exposes every operation in the vCenter Server API so that you can integrate all these operations into your own automated processes.

This chapter includes the following topics:

- Concepts of Workflows
- Performing Administration Tasks on the vSphere Objects
- Configure the Default vRealize Orchestrator
- Managing Associations of Workflows with vSphere Inventory Objects
- Working with Workflows
- Workflows for Managing Inventory Objects

Concepts of Workflows

A workflow is a series of actions and decisions that are automated to run sequentially after you run the workflow. vRealize Orchestrator provides a library of workflows that perform common management tasks.

Basics of Workflows

Workflows consist of a schema, variables, and input and output parameters. The workflow schema is the main component of a workflow as it defines all the workflow elements and the logical task flow of the workflow. The workflow variables and parameters are used by workflows to transfer data. vRealize Orchestrator saves a workflow token every time a workflow runs, recording the details of that specific run of the workflow. This token contains all parameters related to the workflow run. For example, if you run a workflow three times, three workflow tokens are saved.

With the vSphere Client, you can run and schedule workflows on selected objects from the vSphere inventory. You cannot create, delete, edit, and manage workflows in the vSphere Client. You develop and manage workflows in the vRealize Orchestrator client. For more information about the vRealize Orchestrator client, see *Using the VMware vRealize Orchestrator Client*.

Input Workflow Parameters

To run, most workflows require a certain set of input parameters. The workflow processes input parameters that the user, an application, another workflow, or an action passes to it.

For example, if a workflow resets a virtual machine, the workflow requires the name of the virtual machine as an input parameter.

Output Workflow Parameters

The workflow output parameters represent the result from the workflow run. Some workflows and workflow elements can change the output parameters of the workflow when they run. While they run, workflows can receive the output parameters of other workflows as input parameters.

For example, if a workflow creates a snapshot of a virtual machine, the output parameter for the workflow is the resulting snapshot.

Workflow Presentation

When you run a workflow in the vSphere Client, the client loads the workflow presentation. You provide the input parameters of the workflow in the workflow presentation.

Waiting for Input

Some workflows require user input during their run and the run is suspended either until the user provides the required information, or until the workflow run times out.

Performing Administration Tasks on the vSphere Objects

By using the Orchestrator view in the vSphere Client, you can perform administration tasks such as running and scheduling workflows, and viewing the list of available workflows.

From the Orchestrator view in the vSphere Client, you can perform the following tasks:

- Select a default vRealize Orchestrator server.

- Work with workflows. Working with workflows includes the following tasks:

  - Associating workflows with specific vSphere inventory objects such as virtual machines, ESXi hosts, clusters, resource pools, and folders.

  - Exporting and importing existing associations of workflows with vSphere inventory objects for backup purposes or to import them to another vCenter Server instance.

  - Editing associations of workflows with vSphere inventory objects such as virtual machines, ESXi hosts, clusters, resource pools, folders, and others.

- Viewing information about workflow runs and about workflows waiting for user intervention.

- Running and scheduling workflows on vSphere objects.

To run workflows on specific vSphere inventory objects, you must select a default vRealize Orchestrator server. Associate the workflows of the default vRealize Orchestrator server with the vSphere inventory objects that you want to manage.

Configure the Default vRealize Orchestrator

You configure multiple Orchestrator servers to work with a vCenter Server instance that is connected to your vSphere Client. A default Orchestrator server is automatically configured to work with the vCenter Server instance, unless you configure one manually. Otherwise, a default Orchestrator server is automatically selected.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1 Log in to the vSphere Client as a member of the Administrators group.

2 In the object navigator, click **vRealize Operations**.

3 In the **Manage** tab, click the **Servers** subtab.

    A table appears that lists the available vCenter Server instances. Each row of the table contains a vCenter Server and the Orchestrator server that manages it.

4 Click **Edit configuration**.

5 In the **Edit vRealize Orchestrator connections** dialog box, select the default Orchestrator server to manage your vCenter Server instance.

    - Select the **Fixed IP/host name** option and enter the IP address of the Orchestrator server.

    - Select the **Registered as VC extension** option and from the drop-down menu, select the URL address of the Orchestrator server.

6 Click **OK**.

Results

You successfully configured a default vRealize Orchestrator server in the vSphere Client.

Managing Associations of Workflows with vSphere Inventory Objects

You can associate workflows with the different vSphere object types to see more workflows displayed in the context menu when you right-click a vSphere inventory object. You can also run these workflows on more object types.

You can add and edit associations, and export and import XML files containing the associations of workflows with vSphere objects.

Workflows associated with inventory object types are listed in the context menu that appears when you right-click the inventory objects and in the **Actions** menu.

Only users from the Orchestrator Administrator group have the rights to manage the associations of workflows with vSphere inventory objects.

Associate Workflows with vSphere Inventory Object Types

You can associate workflows with a vSphere object type, such as host, to run the workflows directly on the inventory objects of that type.

Workflows associated with inventory object types are listed in the context menu that appears when you right-click an inventory object, and in the **Actions** menu.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

- Log in to the vSphere Client as a member of the Administrators group.

Procedure

1 In the object navigator, click **vRealize Orchestrator**.

2 Click the **Manage** tab.

3 Click the **Context Actions** subtab.

4 Click the **Add** icon ✚ to add a workflow.

5 Select the Orchestrator server from the vRO Servers tree, and navigate through the workflow library to find the workflow to add.

6 Click **Add**.

   The workflow appears in the list of selected workflows on the right.

7   (Optional) Enable multi-selection.

With multi-selection enabled, you can select multiple vSphere objects of the same type when you run the workflow.

8   Under Available types, select the vSphere object types with which you want to associate the workflow.

9   Click **OK**.

Edit the Associations of Workflows with vSphere Objects

You can associate a workflow with different objects from the vSphere inventory and also edit the associations of workflows with the objects from the vSphere inventory.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

- Log in as a member of the Administrators group to configure the default Orchestrator server.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click the **Manage** tab.

3   Click the **Context Actions** subtab.

4   Right-click the workflow to edit and select **Edit**.

5   Change the association properties.

6   Click **OK**.

Export the Associations of Workflows with vSphere Objects

You can transfer the associations of workflows with objects in the vSphere inventory using an XML file.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

- Log in as a member of the Administrators group to configure the default Orchestrator server.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click the **Manage** tab.

3   Click the **Context Actions** subtab.

4   Click the **Export** icon.

5   Select a location where you want to save the XML file, and click **Save**.

Import the Association of Workflows with vSphere Objects

You can import an XML file that contains the association of workflows with objects in the vSphere inventory.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

- Log in as a member of the Administrators group to configure the default Orchestrator server.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click the **Manage** tab.

3   Click the **Context Actions** subtab.

4   Click the **Import** icon.

5   Browse to select the XML file to import and click **Open**.

Results

Orchestrator compares the two associated workflow sets and imports the missing workflow associations.

Working with Workflows

You can view information about Orchestrator workflows, run, and schedule workflows by using the vSphere Client.

You can perform some scheduling and running tasks on the Orchestrator workflows from the vRealize Orchestrator view in the vSphere Client. You can schedule a workflow to run at a specified time or start a workflow directly, by right-clicking a vSphere inventory object and selecting **All vRealize Orchestrator plugin Actions**.

Workflow tasks include:

- Running workflows on vSphere inventory objects, such as virtual machines, ESXi hosts, clusters, resource pools, and folders.

- Viewing information about workflow runs.

- Viewing information about workflows waiting for user interaction.

- Searching for a specific workflow from the list of available workflows.

- Scheduling workflows.

Run Workflows on vSphere Inventory Objects

You can automate management tasks in vSphere by running Orchestrator workflows directly on objects from the vSphere inventory.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

- Verify that you have workflows associated with the vSphere inventory objects. See Associate Workflows with vSphere Inventory Object Types.

Procedure

1 Click **vCenter**.

2 Under Inventory Lists, click an inventory category.

3 Right-click the object that you want to run the workflow on, and navigate to **All vRealize Orchestrator plugin Actions**.

   All available workflows that you can run on the selected inventory object are listed.

4 Click the workflow that you want to run.

   Note If you cannot find the expected workflows, you might need to associate them to the specified vSphere inventory object.

5 Click the **Start/Schedule** menu option.

6 (Optional) Select Run now to start the workflow run immediately.

7   Provide the required workflow parameters.

8   (Optional) Select Schedule to configure the workflow to run at a specified time.

    a   In the **Task name** text box, type the name of the scheduled task.

    b   (Optional) In the **Description** text box, type a description of the scheduled task.

    c   Schedule the date and time of the workflow run.

    d   Specify the recurrence options.

9   Click **Finish**.

View Information About Workflow Runs

You can view information about the workflow runs for each connected Orchestrator server. The available information includes the workflow name, start and end date, state of the workflow, and the user who started the workflow.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

- Run an Orchestrator workflow.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click **vRO Servers**.

    A list of the available vRealize Orchestrator servers appears.

3   Click a vRealize Orchestrator server, and click the **Monitor** tab.

    The list of workflow runs appears.

What to do next

You can review the list of workflow runs, cancel a running workflow, or respond to a workflow that requires interaction.

View Information About the Runs of a Specific Workflow

You can view information about the runs of a single workflow such as start and end date, state of the workflow, and user who has started the workflow.

Prerequisites

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

- Run the specific Orchestrator workflow at least once.

Procedure

1 In the object navigator, click **vRealize Orchestrator**.

2 Under Inventory Lists, click **Workflows**.

 A list of the available workflows appears.

3 Click the name of a workflow, and click the **Monitor** tab.

 A list of workflow runs appears.

What to do next

You can review the list of workflow runs, cancel a running workflow, or respond to a workflow that requires interaction.

View Workflows That Are Waiting for User Interaction

You can view the workflows that are waiting for a user interaction.

Prerequisites

Procedure

1 Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

2 In the object navigator, click **vRealize Orchestrator**.

3 Under Inventory lists, click **Waiting for interaction**.

Results

A list of workflows that are waiting for a user interaction appears.

What to do next

You can provide values for the required parameters of workflows that are waiting for a user interaction.

Searching for Workflows

You can browse for workflows in the inventory of the Orchestrator server or filter the available workflows by a search keyword to find a particular workflow.

Browse the Inventory of the Orchestrator Server

You can view the available workflows in the inventory of each connected Orchestrator server. You can search for a particular type of workflow by browsing the workflow categories.

Prerequisites

Procedure

1   Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*

2   In the object navigator, click **vRealize Orchestrator**.

3   Click **vRO Servers**.

    A list of the available vRealize Orchestrator servers appears

4   Double-click a vRealize Orchestrator server.

5   Click **Categories**.

6   Double-click **Library**.

    Note   **Library** is the default main workflow category. An Orchestrator server can have additional custom workflow categories.

7   Click **Categories**.

    A list of available workflow categories appears.

8   Double-click a workflow category to browse the available workflows and its subcategories.

Find a Workflow

If you have many workflows, you can filter them by a search keyword to find a specific workflow.

Prerequisites

Procedure

1 Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

2 In the object navigator, click **vRealize Orchestrator**.

3 Click **Workflows**.

4 In the **Filter** text box, type a search term or the name of the workflow that you are searching for.

A list displays the workflows that contain the search term in the workflow name or description.

Scheduling Workflows

You can create tasks to schedule workflows, edit scheduled tasks, suspend scheduled tasks, and resume suspended scheduled tasks.

Schedule a Workflow

You can schedule a workflow to run at a specified time. You can also set the recurrence for a scheduled workflow.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1 In the object navigator, click **vRealize Orchestrator**.

2 Under Inventory Lists click **Workflows**.

3 Right-click the workflow that you want to schedule and select **Schedule a workflow**.

4 Provide the required workflow parameters.

5 Click **Start/Schedule**.

6 In the **Task name** text box, type the name of the scheduled task.

7 (Optional) In the **Description** text box, type a description of the scheduled task.

8   Schedule the date and time of the workflow run.

9   Specify the recurrence options.

10 Click **Finish**.

Edit the Schedule of a Workflow

You can modify the schedule of a workflow and set it to run at an earlier or later time.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click **Scheduled workflows**.

A list of the scheduled workflows appears.

3   Right-click the workflow whose schedule you want to edit and select **Edit**.

4   In the **Task name** text box, type the new name of the scheduled task.

5   (Optional) In the **Description** text box, type a description of the scheduled task.

6   Edit the scheduled date and time of the workflow run.

7   Specify the recurrence options.

8   Click **Finish**.

Run a Scheduled Workflow

You can manually run a scheduled workflow before it runs automatically.

When you run a workflow manually, the schedule is not affected. After the manual run, the workflow runs again at the scheduled time.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click **Scheduled workflows**.

A list of the scheduled workflows appears.

3   Click **Scheduled workflows**.

4   Right-click the workflow that you want to run and select **Run now**.

What to do next

You can view information about the workflow run in the Recent Tasks pane or in the Orchestrator server menu. See View Information About Workflow Runs.

Suspend a Scheduled Task

You can suspend a scheduled workflow run. You can also resume suspended scheduled tasks.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1   In the object navigator, click **vRealize Orchestrator**.

2   Click **Scheduled workflows**.

A list of the scheduled workflows appears.

3   Right-click a workflow and select **Suspend**.

The workflow schedule is suspended.

Results

The state of the scheduled task changes to Suspended.

Resume a Suspended Scheduled Task

You can resume a scheduled task that has been suspended.

Prerequisites

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Procedure

1 In the object navigator, click **vRealize Orchestrator**.

2 Click **Scheduled workflows**.

   A list of the scheduled workflows appears.

3 Right-click a workflow and select **Resume**.

   The workflow schedule is resumed from suspension.

Results

The state of the scheduled task changes to Pending.

Workflows for Managing Inventory Objects

The default workflows for managing vSphere inventory objects are the workflows included in the vCenter Server plug-in workflow library. The vCenter Server plug-in workflow library contains workflows that you can use to run automated processes related to the vCenter Server and host management.

To access workflows in the vSphere Client, make sure that you configure at least one running Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize Orchestrator*.

Note Only a predefined set of vCenter Server workflows are available by default in the context menu. You can associate additional workflows with each vSphere object. See Associate Workflows with vSphere Inventory Object Types.

Cluster and Compute Resource Workflows

With the cluster and compute resource workflows, you can create, rename or delete a cluster, and enable or disable high availability on a cluster.

Add DRS virtual machine group to cluster

Adds a DRS virtual machine group to a cluster.

Add virtual machines to DRS group

Adds a virtual machine list to an existing DRS virtual machine group.

Create cluster

Creates a cluster in a host folder.

Delete cluster

Deletes a cluster.

Disable DRS on cluster

Disables DRS on a cluster.

Disable HA on cluster

Disables high availability on a cluster.

Disable vCloud Distributed Storage on cluster

Disables vCloud Distributed Storage on a cluster.

Enable DRS on cluster

Enables DRS on a cluster.

Enable HA on cluster

Enables high availability on a cluster.

Enable vCloud Distributed Storage on cluster

Enables vCloud Distributed Storage on a cluster.

Remove virtual machine DRS group from cluster

Removes a DRS virtual machine group from a cluster.

Remove virtual machines from DRS group

Removes virtual machines from a cluster DRS group.

Rename cluster

Renames a cluster.

Guest Operation Files Workflows

With the guest operation files workflows, you can manage files in a guest operating system.

Check for directory in guest

> Verifies that a directory exists in a guest virtual machine.

Check for file in guest

> Verifies that a file exists in a guest virtual machine.

Copy file from guest to Orchestrator

> Copies a specified file from a guest file system to an Orchestrator server.

Copy file from Orchestrator to guest

> Copies a specified file from an Orchestrator server to a guest file system.

Create directory in guest

> Creates a directory in a guest virtual machine.

Create temporary directory in guest

> Creates a temporary directory in a guest virtual machine.

Create temporary file in guest

> Creates a temporary file in a guest virtual machine.

Delete directory in guest

> Deletes a directory from a guest virtual machine.

Delete file in guest

> Deletes a file from a guest virtual machine.

List path in guest

> Shows a path in a guest virtual machine.

Move directory in guest

> Moves a directory in a guest virtual machine.

Move file in guest

> Moves a file in a guest virtual machine.

Guest Operation Processes Workflows

With the guest operation processes workflows, you can get information and control the running processes in a guest operating system.

Get environment variables from guest

> Returns a list with environmental variables from a guest. An interactive session returns the variables of the user who is logged in.

Get processes from guest

Returns a list with the processes running in the guest operating system and the recently completed processes started by the API.

Run program in guest

Starts an application in a guest operating system.

Kill process in guest

Terminates a process in a guest operating system.

Custom Attributes Workflows

With the custom attributes workflows, you can add custom attributes to virtual machines or get a custom attribute for a virtual machine.

Add custom attribute to a virtual machine

Adds a custom attribute to a virtual machine.

Add custom attribute to multiple virtual machines

Adds a custom attribute to a selection of virtual machines.

Get custom attribute

Gets a custom attribute for a virtual machine in vCenter Server.

Data Center Workflows

With the data center workflows, you can create, delete, reload, rename, or rescan a data center.

Create datacenter

Creates a data center in a data center folder.

Delete datacenter

Deletes a data center.

Reload datacenter

Forces vCenter Server to reload data from a data center.

Rename datacenter

Renames a data center and waits for the task to complete.

Rescan datacenter HBAs

Scans the hosts in a data center and initiates a rescan on the host bus adapters to discover new storage.

Datastore and Files Workflows

With the datastore and files workflows, you can delete a list of files, find unused files in a datastore, and others.

Delete all files

Deletes a list of files.

Delete all unused datastore files

Searches all datastores in the vCenter Server environment and deletes all unused files.

Export unused datastore files

Searches all datastores and creates an XML descriptor file that lists all unused files.

Find unused files in datastores

Searches the vCenter Server environment for all unused disks (`*.vmdk`), virtual machines (`*.vmx`), and template (`*.vmtx`) files that are not associated with any vCenter Server instances registered with Orchestrator.

Get all configuration, template, and disk files from virtual machines

Creates a list of all virtual machine descriptor files and a list of all virtual machine disk files, for all datastores.

Log all datastore files

Creates a log for every virtual machine configuration file and every virtual machine file found in all datastores.

Log unused datastore files

Searches the vCenter Server environment for unused files that are registered on virtual machines and exports a log of the files in a text file.

Upload file to datastore

Uploads a file to an existing folder on a specific datastore. The uploaded file overwrites any existing file with the same name in the same destination folder.

Data Center Folder Management Workflows

With the data center folder management workflows, you can create, delete, or rename a data center folder.

Create datacenter folder

Creates a data center folder.

Delete datacenter folder

Deletes a data center folder and waits for the task to complete.

Rename datacenter folder

Renames a data center folder and waits for the task to complete.

Host Folder Management Workflows

With the host folder management workflows, you can create, delete, or rename a host folder.

Create host folder

Creates a host folder.

Delete host folder

Deletes a host folder and waits for the task to complete.

Rename host folder

Renames a host folder and waits for the task to complete.

Virtual Machine Folder Management Workflows

With the virtual machine folder management workflows, you can create, delete, or rename a virtual machine folder.

Create virtual machine folder

Creates a virtual machine folder.

Delete virtual machine folder

Deletes a virtual machine folder and waits for the task to complete.

Rename virtual machine folder

Renames a virtual machine folder and waits for the task to complete.

Basic Host Management Workflows

With the basic host management workflows, you can put a host into maintenance mode, make a host exit maintenance mode. You can also move a host to a folder or a cluster, and reload data from a host.

Enter maintenance mode

Puts the host into maintenance mode. You can cancel the task.

Exit maintenance mode

Exits maintenance mode. You can cancel the task.

Move host to cluster

Moves an existing host into a cluster. The host must be part of the same data center, and if the host is part of a cluster, the host must be in maintenance mode.

Move host to folder

Moves a host into a folder as a standalone host. The host must be part of a ClusterComputeResource in the same data center and the host must be in maintenance mode.

Reload host

Forces vCenter Server to reload data from a host.

Host Power Management Workflows

With the host power management workflows, you can reboot or shut down a host.

Reboot host

Reboots a host. If the Orchestrator client is connected directly to the host, it loses the connection to the host and does not receive an indication of success in the returned task.

Shut down host

Shuts down a host. If the Orchestrator client is connected directly to the host, it loses the connection to the host and does not receive an indication of success in the returned task.

Host Registration Management Workflows

With the host registration management workflows, you can add a host to a cluster, disconnect or reconnect a host from a cluster, and others.

Add host to cluster

Adds a host to the cluster. This workflow fails if it cannot authenticate the SSL certificate of the host.

Add standalone host

Registers a host as a standalone host.

Disconnect host

Disconnects a host from vCenter Server.

Reconnect host

Reconnects a disconnected host by providing only the host information.

Reconnect host with all information

Reconnects a disconnected host by providing all information about the host.

Remove host

Removes a host and unregisters it from vCenter Server. If the host is part of a cluster, you must put it in maintenance mode before attempting to remove it.

Networking Workflows

With the networking workflows, you can add a port group to distributed virtual switch, create a distributed virtual switch with a port group, and others.

Add port group to distributed virtual switch

Adds a new distributed virtual port group to a specified distributed virtual switch.

Attach host system to distributed virtual switch

Adds a host to a distributed virtual switch.

Create distributed virtual switch with port group

Creates a distributed virtual switch with a distributed virtual port group.

Distributed Virtual Port Group Workflows

With the distributed virtual port group workflows, you can update or delete a port group, and reconfigure the port group.

Connect virtual machine NIC number to distributed virtual port group

Reconfigures the network connection of the specified virtual machine NIC number to connect to the specified distributed virtual port group. If no NIC number is specified, the number zero is used.

Delete distributed virtual port group

Deletes a specified distributed virtual port group.

Set teaming options

Provides an interface to manage the teaming options for a distributed virtual port group.

Update distributed virtual port group

Updates the configuration of a specified distributed virtual port group.

Distributed Virtual Switch Workflows

With the distributed virtual switch workflows, you can create, update, or delete a distributed virtual switch, and create, delete, or update a private VLAN.

Create distributed virtual switch

Creates a distributed virtual switch in the specified network folder with a name and uplink port names that you specify. You must specify at least one uplink port name.

Create private VLAN

Creates a VLAN on the specified distributed virtual switch.

Delete distributed virtual switch

Deletes a distributed virtual switch and all associated elements.

Delete private VLAN

Deletes a VLAN from a specified distributed virtual switch. If a secondary VLAN exists, you must first delete the secondary VLAN.

Update distributed virtual switch

Updates the properties of a distributed virtual switch.

Update private VLAN

Updates a VLAN on the specified distributed virtual switch.

Standard Virtual Switch Workflows

With the standard virtual switch workflows, you can create, update, or delete a standard virtual switch, and create, delete, or update port groups in standard virtual switches.

Add port group in standard virtual switch

Adds a port group in a standard virtual switch.

Create standard virtual switch

Creates a standard virtual switch.

Delete port group from standard virtual switch

Deletes a port group from a standard virtual switch.

Delete standard virtual switch

Deletes a standard virtual switch from a host's network configuration.

Retrieve all standard virtual switches

Retrieves all standard virtual switches from a host.

Update port group in standard virtual switch

Updates the properties of a port group in a standard virtual switch.

Update standard virtual switch

Updates the properties of a standard virtual switch.

Update vNIC for port group in standard virtual switch

Updates a vNIC associated with a port group in a standard virtual switch.

Resource Pool Workflows

With the resource pool workflows, you can create, rename, reconfigure or delete a resource pool, and get resource pool information.

Create resource pool

Creates a resource pool with the default CPU and memory allocation values. To create a resource pool in a cluster, the cluster must have VMware DRS enabled.

Create resource pool with specified values

Creates a resource pool with CPU and memory allocation values that you specify. To create a resource pool in a cluster, the cluster must have VMware DRS enabled.

Delete resource pool

Deletes a resource pool and waits for the task to complete.

Get resource pool information

Returns CPU and memory information about a given resource pool.

Reconfigure resource pool

Reconfigures CPU and memory allocation configuration for a given resource pool.

Rename resource pool

Renames a resource pool and waits for the task to complete.

Storage Workflows

With the storage workflows, you can perform storage-related operations.

Add datastore on iSCSI/FC/local SCSI

Creates a datastore on a Fibre Channel, iSCSI or local SCSI disk. Only disks that are not in use by an existing VMFS are applicable to new datastore creation. The new datastore allocates the maximum available space of the specified disk.

Add datastore on NFS

Adds a datastore on an NFS server.

Add iSCSI target

Adds iSCSI targets to a vCenter Server host. The targets can be of the type `Send` or `Static.`

Create VMFS for all available disks

Creates a VMFS volume for all available disks of a specified host.

Delete datastore

Deletes datastores from a vCenter Server host.

Delete iSCSI target

Deletes already configured iSCSI targets. The targets can be of type `Send` or `Static.`

Disable iSCSI adapter

Disables the software iSCSI adapter of a specified host.

Display all datastores and disks

Displays the existing datastores and available disks on a specified host.

Enable iSCSI adapter

Enables an iSCSI adapter.

List all storage adapters

Lists all storage adapters of a specified host.

Storage DRS Workflows

With the storage DRS workflows, you perform storage-related operations. These include creating and configuring a datastore cluster, removing a datastore from a cluster, adding storage to a cluster, and others.

Add datastore to cluster

Adds datastores to a datastore cluster. Datastores must be able to connect to all hosts to be included in the datastore cluster. Datastores must have the same connection type to reside within a datastore cluster.

Change Storage DRS per virtual machine configuration

Sets Storage DRS settings for each virtual machine.

Configure datastore cluster

Configures datastore cluster setting values for automation and runtime rules.

Create simple datastore cluster

Creates a simple datastore cluster with default configuration. The new datastore cluster contains no datastores.

Create Storage DRS scheduled task

Creates a scheduled task for reconfiguring a datastore cluster. Only automation and runtime rules can be set.

Create virtual machine anti-affinity rule

Creates an anti-affinity rule to indicate that all virtual disks of certain virtual machines must be kept on different datastores.

Create VMDK anti-affinity rule

Creates a VMDK anti-affinity rule for a virtual machine that indicates which of its virtual disks must be kept on different datastores. The rule applies to the virtual disks of the selected virtual machine.

Remove datastore cluster

Removes a datastore cluster. Removing a datastore cluster also removes all the settings and the alarms for the cluster from the vCenter Server system.

Remove datastore from cluster

Removes a datastore from a datastore cluster and puts the datastore in a datastore folder.

Remove Storage DRS scheduled task

Removes a scheduled Storage DRS task.

Remove virtual machine anti-affinity rule

Removes a virtual machine anti-affinity rule for a given datastore cluster.

Remove VMDK anti-affinity rule

Removes a VMDK anti-affinity rule for a given datastore cluster.

Basic Virtual Machine Management Workflows

With the basic virtual machine management workflows, you can perform basic operations on virtual machines, for example, create, rename, or delete a virtual machine, upgrade virtual hardware, and others.

Create custom virtual machine

Creates a virtual machine with the specified configuration options and additional devices.

Create simple dvPortGroup virtual machine

Creates a simple virtual machine. The network used is a Distributed Virtual Port Group.

Create simple virtual machine

Creates a virtual machine with the most common devices and configuration options.

Delete virtual machine

Removes a virtual machine from the inventory and datastore.

Get virtual machines by name

Returns a list of virtual machines from all registered vCenter Server instances that match the provided expression.

Mark as template

Converts an existing virtual machine to a template, not allowing it to start. You can use templates to create virtual machines.

Mark as virtual machine

Converts an existing template to a virtual machine, allowing it to start.

Move virtual machine to folder

Moves a virtual machine to a specified virtual machine folder.

Move virtual machine to resource pool

Moves a virtual machine to a resource pool. If the target resource pool is not in the same cluster, you must use the migrate or relocate workflows.

Move virtual machines to folder

Moves several virtual machines to a specified virtual machine folder.

Move virtual machines to resource pool

Moves several virtual machines to a resource pool.

Register virtual machine

Registers a virtual machine. The virtual machine files must be placed in an existing datastore and must not be already registered.

Reload virtual machine

Forces vCenter Server to reload a virtual machine.

Rename virtual machine

Renames an existing virtual machine on the vCenter Server system or host and not on the datastore.

Set virtual machine performance

Changes performance settings such as shares, minimum and maximum values, shaping for network, and disk access of a virtual machine.

Unregister virtual machine

Removes an existing virtual machine from the inventory.

Upgrade virtual machine hardware (force if required)

Upgrades the virtual machine hardware to the latest revision that the host supports. This workflow forces the upgrade to continue, even if VMware Tools is out of date. If the VMware Tools is out of date, forcing the upgrade to continue reverts the guest network settings to the default settings. To avoid this situation, upgrade VMware Tools before running the workflow.

Upgrade virtual machine

Upgrades the virtual hardware to the latest revision that the host supports. An input parameter allows a forced upgrade even if VMware Tools is out of date.

Wait for task and answer virtual machine question

Waits for a vCenter Server task to complete or for the virtual machine to ask a question. If the virtual machine requires an answer, accepts user input and answers the question.

Clone Workflows

With the clone workflows, you can clone virtual machines with or without customizing the virtual machine properties.

Clone virtual machine from properties

Clones virtual machines by using properties as input parameters.

Clone virtual machine, no customization

Clones a virtual machine without changing anything except the virtual machine UUID.

Customize virtual machine from properties

Customizes a virtual machine by using properties as input parameters.

Linked Clone Workflows

With the linked clone workflows, you can perform linked clone operations, such as restoring a virtual machine from a linked clone, creating a linked clone, and others.

Restore virtual machine from linked clone

Removes a virtual machine from a linked clone setup.

Set up virtual machine for linked clone

Prepares a virtual machine to be link cloned.

Create a linked clone of a Linux machine with multiple NICs

Creates a linked clone of a Linux virtual machine, performs the guest operating system customization, and configures up to four virtual network cards.

Create a linked clone of a Linux machine with a single NIC

Creates a linked clone of a Linux virtual machine, performs the guest operating system customization, and configures one virtual network card.

Create a linked clone of a Windows machine with multiple NICs and credential

Creates a linked clone of a Windows virtual machine and performs the guest operating system customization. Configures up to four virtual network cards and a local administrator user account.

Create a linked clone of a Windows machine with a single NIC and credential

Creates a linked clone of a Windows virtual machine and performs the guest operating system customization. Configures one virtual network card and a local administrator user account.

Create a linked clone with no customization

Creates the specified number of linked clones of a virtual machine.

Linux Customization Clone Workflows

With the Linux customization workflows, you can clone a Linux virtual machine and customize the guest operating system.

Clone a Linux machine with multiple NICs

Clones a Linux virtual machine, performs the guest operating system customization, and configures up to four virtual network cards.

Clone a Linux machine with a single NIC

Clones a Linux virtual machine, performs the guest operating system customization, and configures one virtual network card.

Tools Clone Workflows

Use the tools clone workflows to obtain information about customizing the operating system of a virtual machine, updating a virtual device, and so on.

Get a virtual Ethernet card to change the network

Returns a new Ethernet card to update a virtual device. Contains only the device key of the given virtual device and the new network.

Get Linux customization

Returns the Linux customization preparation.

Get multiple virtual Ethernet card device changes

Returns an array of VirtualDeviceConfigSpec objects for add and remove operations on VirtualEthernetCard objects.

Get NIC setting map

Returns the setting map for a virtual network card by using VimAdapterMapping.

Get Windows customization for Sysprep with credentials

Returns customization information about the Microsoft Sysprep process, with credentials. Workflows for cloning Windows virtual machines use this workflow.

Get Windows customization for Sysprep with Unattended.txt

Returns customization information about the Microsoft Sysprep process by using an Unattended.txt file. Workflows for cloning Windows virtual machines use this workflow.

Get Windows customization for Sysprep

Returns customization information about the Microsoft Sysprep process. Workflows for cloning Windows virtual machines use this workflow.

Windows Customization Clone Workflows

With the Windows customization clone workflows, you can clone Windows virtual machines and customize the guest operating system.

Customize a Windows machine with single NIC and credential

Performs guest operating system customization, configures one virtual network card and a local administrator user account on a Windows virtual machine.

Clone a thin provisioned Windows machine with single NIC and credential

Clones a Windows virtual machine performing the guest operating system customization. Specifies virtual disk thin provisioning policy and configures one virtual network card and a local administrator user account. Sysprep tools must be available on the vCenter Server system.

Clone a Windows machine Sysprep with single NIC and credential

Clones a Windows virtual machine performing the guest operating system customization. Configures one virtual network card and a local administrator user account. Sysprep tools must be available on vCenter Server.

Clone a Windows machine with multiple NICs and credential

Clones a Windows virtual machine performing the guest operating system customization. Configures the local administrator user account and up to four virtual network cards. Sysprep tools must be available on the vCenter Server system.

Clone a Windows machine with single NIC

Clones a Windows virtual machine performing the guest operating system customization and configures one virtual network card. Sysprep tools must be available on the vCenter Server system.

Clone a Windows machine with single NIC and credential

Clones a Windows virtual machine performing the guest operating system customization. Configures one virtual network card and a local administrator user account. Sysprep tools must be available on the vCenter Server system.

Device Management Workflows

With the device management workflows, you can manage the devices that are connected to a virtual machine or to a datastore of a host.

Add CD-ROM

Adds a virtual CD-ROM to a virtual machine. If the virtual machine has no IDE controller, the workflow creates one.

Add disk

Adds a virtual disk to a virtual machine.

Change RAM

Changes the amount of RAM of a virtual machine.

Convert disks to thin provisioning

Converts thick-provisioned disks of virtual machines to thin-provisioned disks.

Convert independent disks

Converts all independent virtual machine disks to normal disks by removing the independent flag from the disks.

Disconnect all detachable devices from a running virtual machine

Disconnects floppy disks, CD-ROM drives, parallel ports, and serial ports from a running virtual machine.

Mount CD-ROM

Mounts the CD-ROM of a virtual machine. If the virtual machine has no IDE controller or CD-ROM drive, the workflow creates them.

Mount floppy disk drive

Mounts a floppy disk drive FLP file from the ESX datastore.

Move and Migrate Workflows

With the move and migrate workflows, you can migrate virtual machines.

Mass migrate virtual machines with Storage vMotion

Uses Storage vMotion to migrate a single virtual machine, a selection of virtual machines, or all available virtual machines.

Mass migrate virtual machines with vMotion

Uses vMotion, Storage vMotion, or both vMotion and Storage vMotion to migrate a single virtual machine, a selection of virtual machines, or all available virtual machines.

Migrate virtual machine with vMotion

Migrates a virtual machine from one host to another by using the `MigrateVM_Task` operation from the vSphere API.

Move virtual machine to another vCenter Server system

Moves a list of virtual machines to another vCenter Server system.

Quick migrate multiple virtual machines

Suspends the virtual machines if they are powered on and migrates them to another host using the same storage.

Quick migrate virtual machine

Suspends the virtual machine if it is powered on and migrates it to another host using the same storage.

Relocate virtual machine disks

Relocates virtual machine disks to another host or datastore while the virtual machine is powered off by using the `RelocateVM_Task` operation from the vSphere API.

Other Workflows

With the workflows in the Others category, you can enable and disable Fault Tolerance (FT), extract virtual machine information, and find orphaned virtual machines.

Disable FT

Disables Fault Tolerance for a specified virtual machine.

Enable FT

Enables Fault Tolerance for a specified virtual machine.

Extract virtual machine information

Returns the virtual machine folder, host system, resource pool, compute resource, datastore, hard drive sizes, CPU and memory, network, and IP address for a given virtual machine. Might require VMware Tools.

Find orphaned virtual machines

Lists all virtual machines in an orphaned state in the Orchestrator inventory. Lists the VMDK and VMTX files for all datastores in the Orchestrator inventory that have no association with any virtual machines in the Orchestrator inventory. Sends the lists by email (optional).

Get Virtual Machine by Name and BIOS UUID

Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) to identify a unique virtual machine.

Note   This workflow is needed when DynamicOps calls vRealize Orchestrator workflows having input parameters of `VC:VirtualMachine` type to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.

Get Virtual Machine by Name and UUID

Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) to identify a unique virtual machine.

Note   This workflow is needed when DynamicOps calls vRealize Orchestrator workflows having input parameters of `VC:VirtualMachine` type to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.

Get Virtual Machine UUID

Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) to identify a unique virtual machine.

Note   This workflow is needed when DynamicOps calls vRealize Orchestrator workflows having input parameters of `VC:VirtualMachine` type to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.

Power Management Workflows

With the power management workflows, you can power on and off virtual machines, reboot the guest operating system of a virtual machine, suspend a virtual machine, and others.

Power off virtual machine and wait

Powers off a virtual machine and waits for the process to complete.

Reboot guest OS

Reboots the virtual machine's guest operating system. Does not reset nonpersistent virtual machines. VMware Tools must be running.

Reset virtual machine and wait

Resets a virtual machine and waits for the process to complete.

Resume virtual machine and wait

Resumes a suspended virtual machine and waits for the process to complete.

Set guest OS to standby mode

Sets the guest operating system to standby mode. VMware Tools must be running.

Shut down and delete virtual machine

Shuts down a virtual machine and deletes it from the inventory and disk.

Shut down guest OS and wait

Shuts down a guest operating system and waits for the process to complete.

Start virtual machine and wait

Starts a virtual machine and waits for VMware Tools to start.

Suspend virtual machine and wait

Suspends a virtual machine and waits for the process to complete.

Snapshot Workflows

With the snapshot workflows, you can perform snapshot-related operations.

Create a snapshot

Creates a snapshot.

Create snapshots of all virtual machines in a resource pool

Creates a snapshot of each virtual machine in a resource pool.

Remove all snapshots

Removes all existing snapshots without reverting to a previous snapshot.

Remove excess snapshots

Finds virtual machines with more than a given number of snapshots and optionally deletes the oldest snapshots. Sends the results by email.

Remove old snapshots

Gets all snapshots that are older than a given number of days and prompts the user to select which ones to delete.

Remove snapshots of a given size

Gets all snapshots that are larger than a given size and prompts the user to confirm deletion.

Revert to current snapshot

Reverts to the current snapshot.

Revert to snapshot and wait

Reverts to a specific snapshot. Does not delete the snapshot.

VMware Tools Workflows

With the VMware Tools workflows, you can perform VMware Tools-related tasks on virtual machines.

Mount VMware tools installer

Mounts the VMware Tools installer on the virtual CD-ROM.

Set console screen resolution

Sets the console window's resolution. The virtual machine must be powered on.

Turn on time synchronization

Turns on time synchronization between the virtual machine and the ESX server in VMware Tools.

Unmount VMware tools installer

Unmounts the VMware Tools CD-ROM.

Upgrade VMware tools

Upgrades VMware Tools on a virtual machine.

Upgrade VMware tools at next reboot

Upgrades VMware Tools on a virtual machine without performing an automatic reboot.

About Headless Systems

15

ESXi supports the detection and configuration of headless systems.

A headless system is a system that can be operated without a monitor, keyboard, or mouse. Network Appliance boxes do not have VGA, the primary interface is a single serial port. You can set up your existing headless systems to use ESXi. You can add ESXi appliances to a data center where virtual machines are managed with vSphere Virtual Center. All existing ESXi features can be used with a headless system that is configured with either embedded flash or minimal local storage. ESXi allows for dynamic switching between different serial modes, which is useful for diagnosing and debugging problems. You can switch between modes to view or modify system parameters.

This chapter includes the following topics:

- Detecting a Headless System
- About Serial Mode Dynamic Switching

Detecting a Headless System

ESXi automatically detects headless systems.

ESXi automatically redirects the DCUI over a serial port connection to improve headless detection. When ESXi automatically detects a headless system, ESXi will set up the serial port as COM1, 115200 baud, and redirects the DCUI over this serial port. The specific settings of com port and baud rate are read from the SPCR (Serial Port Console Redirection) table, if it exists. This behavior can be disabled using new boot parameters if the default settings are not acceptable. You can set the `headless` flag in the ACPI FADT table to mark a system as headless.

About Serial Mode Dynamic Switching

ESXi supports dynamic switching between four different serial port modes.

ESXi supports serial mode dynamic switching to provide maximum platform flexibility, and to allow debugging and supportability in the text box. ESXi examines the input characters for any serial port mode and switches the modes based on the input key sequence. DCUI, Shell, GDB, and Logging modes are supported. If you have two serial ports, only one of the four modes is

allowed on each port. Two serial ports cannot be in the same mode. If you attempt a dynamic switch to a mode in use by the other serial port, the request is ignored. Dynamic switching eliminates the need to interrupt the boot process manually or to create a custom image to redirect to a serial port. It also addresses supportability issues regarding headless systems that only have one serial port, by making it possible to switch the serial port between different modes of operation.

ESXi Serial Port Modes

ESXi supports four serial port modes.

There are four serial port modes in ESXi:

Logging mode – Logging mode is the default mode in a debug build. Logging mode sends the vmkernel.log over the serial port.

GDB mode – Use GDB mode for dedicated debugging.

Shell mode – Shell mode is the shell port access, which is similar to SSH.

DCUI mode – DCUI mode is a Direct Console User Interface. This is the user interface that is displayed when you boot ESXi using a monitor.

Note   Only COM1 and COM2 ports are supported. USB serial or PCI serial cards are not supported.

Dynamic Switching Keystrokes

ESXi includes a unique keystroke sequence that allows dynamic serial mode switching.

Dynamic Switching Keystrokes

Once the correct keystroke sequence is entered, the system switches the serial port to the desired mode.

Logging mode: `Ctrl+G, Ctrl+B, 1`

Shell mode: `Ctrl+G, Ctrl+B, 2`

DCUI mode: `Ctrl+G, Ctrl+B, 3`

GDB mode: `Ctrl+G, Ctrl+B, ?`

Note   Once in GDB mode, you cannot switch modes again using a key sequence. You must use the CLI to switch modes.

Serial Port Dynamic Switching Using the CLI

You can switch serial modes using the CLI.

Dynamic Switching Using the CLI

Use esxcfg-advcfg to set the current mode to **none**. Then set the new desired mode using the CLI.

Logging mode: `esxcfg—advcfg —s com1 /Misc/LogPort`

Shell mode: `esxcfg—advcfg —s com1 /Misc/ShellPort`

DCUI mode: `esxcfg—advcfg —s com1 /Misc/ConsolePort`

GDB mode: `esxcfg—advcfg —s com1 /Misc/GDBPort`

Example: Example

If the serial mode is set to logging mode, enter these two commands to switch it to DCUI mode.

`§. > esxcfg—advcfg -s none /Misc/LogPort`

`§. > esxcfg—advcfg -s com1 /Misc/ConsolePort`

Controlling the Serial DCUI

You can use alternate keystrokes to control the DCUI over a serial port. These alternate are useful when F2 or other function keys cannot be used.

Controlling the Serial DCUI

Alternate keystroke mappings for DCUI mode:

- Esc + 1 -> F1

- Esc + 2 -> F2

- Esc + 3 -> F3

- Esc + 4 -> F4

- Esc + 5 -> F5

- Esc + 6 -> F6

- Esc + 7 -> F7

- Esc + 8 -> F8

- Esc + 9 -> F9

- Esc + 0 -> F10

- Esc + ! -> F11

- Esc + @ -> F12

Troubleshooting Overview

<div style="text-align: right; font-size: 3em; color: gray;">16</div>

vSphere Troubleshooting contains common troubleshooting scenarios and provides solutions for each of these problems. You can also find guidance here for resolving problems that have similar origins. For unique problems, consider developing and adopting a troubleshooting methodology.

The following approach for effective troubleshooting elaborates on how to gather troubleshooting information, such as identifying symptoms and defining the problem space. Troubleshooting with log files is also discussed.

This chapter includes the following topics:

- Troubleshooting vCenter Server
- Troubleshooting vCenter Server and ESXi Host Certificates
- Troubleshooting Hosts
- Troubleshooting Licensing

Troubleshooting vCenter Server

These troubleshooting topics provide solutions to problems you might encounter in vCenter Server.

Guidelines for Troubleshooting

To troubleshoot your implementation of vSphere, identify the symptoms of the problem, determine which of the components are affected, and test possible solutions.

Identifying Symptoms

A number of potential causes might lead to the under-performance or nonperformance of your implementation. The first step in efficient troubleshooting is to identify exactly what is going wrong.

Defining the Problem Space

After you have isolated the symptoms of the problem, you must define the problem space. Identify the software or hardware components that are affected and might be causing the problem and those components that are not involved.

Testing Possible Solutions

When you know what the symptoms of the problem are and which components are involved, test the solutions systematically until the problem is resolved.

Troubleshooting Basics
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_troubleshooting)

Identifying Symptoms

Before you attempt to resolve a problem in your implementation, you must identify precisely how it is failing.

The first step in the troubleshooting process is to gather information that defines the specific symptoms of what is happening. You might ask these questions when gathering this information:

- What is the task or expected behavior that is not occurring?

- Can the affected task be divided into subtasks that you can evaluate separately?

- Is the task ending in an error? Is an error message associated with it?

- Is the task completing but in an unacceptably long time?

- Is the failure consistent or sporadic?

- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space

After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings

- Failure of physical hardware

- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions

After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.

- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.

- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.

- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.

- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.

- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Troubleshooting with Logs

You can often obtain valuable troubleshooting information by looking at the logs provided by the various services and agents that your implementation is using.
Most logs are located in `/var/log/` for vCenter Server deployments.

Common Logs

The following logs are common to all vCenter Server deployments.

Table 16-1. Common Log Directories

Log Directory	Description
vmware/applmgmt	VMware Appliance Management Service
cloudvm	Logs for allotment and distribution of resources between services
firstboot	Location where first boot logs are stored
rhttpproxy	Reverse Web Proxy
sca	VMware Service Control Agent
vmware/applmgmt	VMware Appliance Monitoring Service
vapi	VMware vAPI Endpoint
vmafdd	VMware Authentication Framework daemon
vmdird	VMware Directory Service daemon
vmon	VMware Service Lifecycle Manager

Management Node Logs

The following logs are available if a management node deployment is chosen.

Table 16-2. Management Node Log Directories

Log Directory	Description
vmware/rbd	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
netdumper	VMware vSphere ESXi Dump Collector
perfcharts	VMware Performance Charts
vmcam	VMware vSphere Authentication Proxy
vmdird	VMware Directory Service daemon
vmware-sps	VMware vSphere Profile-Driven Storage Service
vpxd	VMware VirtualCenter Server
vpostgres	vFabric Postgres database service
vcha	VMware High Availability Service

vCenter Server Upgrade Fails When Unable to Stop Tomcat Service

A vCenter Server upgrade can fail when the installer is unable to stop the Tomcat service.

Problem

If the vCenter Server installer cannot stop the Tomcat service during an upgrade, the upgrade fails with an error message similar to `Unable to delete VC Tomcat service`. This problem can occur even if you stop the Tomcat service manually before the upgrade, if some files that are used by the Tomcat process are locked.

Solution

1   From the Windows **Start** menu, select **Settings > Control Panel > Administrative Tools > Services**.

2   Right-click **VMware VirtualCenter Server** and select **Manual**.

3   Right-click **VMware vCenter Management Webservices** and select **Manual**.

4   Reboot the vCenter Server machine before upgrading.

    This releases any locked files that are used by the Tomcat process, and enables the vCenter Server installer to stop the Tomcat service for the upgrade.

Solution

Alternatively, you can restart the vCenter Server machine and restart the upgrade process, but select the option not to overwrite the vCenter Server data.

Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail

vCenter Server installation with a Microsoft SQL database fails when the database is set to compatibility mode with an unsupported version.

Problem

The following error message appears: `The DB User entered does not have the required permissions needed to install and configure vCenter Server with the selected DB. Please correct the following error(s): %s`

Cause

The database version must be supported for vCenter Server. For SQL, even if the database is a supported version, if it is set to run in compatibility mode with an unsupported version, this error occurs. For example, if SQL 2008 is set to run in SQL 2000 compatibility mode, this error occurs.

Solution

◆   Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version. See the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Troubleshooting vCenter Server and ESXi Host Certificates

Certificates are automatically generated when you install vCenter Server. These default certificates are not signed by a commercial certificate authority (CA) and might not provide strong security. You can replace default vCenter Server certificates with certificates signed by a commercial CA. When you replace vCenter Server and ESXi certificates, you might encounter errors.

New vCenter Server Certificate Does Not Appear to Load

After you replace default vCenter Server certificates, the new certificates might not appear to load.

Problem

When you install new vCenter Server certificates, you might not see the new certificate.

Cause

Existing open connections to vCenter Server are not forcibly closed and might still use the old certificate.

Solution

To force all connections to use the new certificate, use one of the following methods.

- Restart the network stack or network interfaces on the server.

- Restart the vCenter Server service.

vCenter Server Cannot Connect to Managed Hosts

After you replace default vCenter Server certificates and restart the system, vCenter Server might not be able to connect to managed hosts.

Problem

vCenter Server cannot connect to managed hosts after server certificates are replaced and the system is restarted.

Solution

Log into the host as the root user and reconnect the host to vCenter Server.

Troubleshooting Hosts

The host troubleshooting topics provide solutions to potential problems that you might encounter when using your vCenter Servers and ESXi hosts.

Troubleshooting vSphere HA Host States

vCenter Server reports vSphere HA host states that indicate an error condition on the host. Such errors can prevent vSphere HA from fully protecting the virtual machines on the host and can impede vSphere HA's ability to restart virtual machines after a failure. Errors can occur when vSphere HA is being configured or unconfigured on a host or, more rarely, during normal operation. When this happens, you should determine how to resolve the error, so that vSphere HA is fully operational.

vSphere HA Agent Is in the Agent Unreachable State

The vSphere HA agent on a host is in the Agent Unreachable state for a minute or more. User intervention might be required to resolve this situation.

Problem

vSphere HA reports that an agent is in the Agent Unreachable state when the agent for the host cannot be contacted by the primary host or by vCenter Server. Consequently, vSphere HA is not able to monitor the virtual machines on the host and might not restart them after a failure.

Cause

A vSphere HA agent can be in the Agent Unreachable state for several reasons. This condition most often indicates that a networking problem is preventing vCenter Server or the primary host from contacting the agent on the host, or that all hosts in the cluster have failed. This condition can also indicate the unlikely situation that vSphere HA was disabled and then re-enabled on the cluster while vCenter Server could not communicate with the vSphere HA agent on the host, or that the ESXi host agent on the host has failed, and the watchdog process was unable to restart it. In any of these cases, a failover event is not triggered when a host goes into the Unreachable state.

Solution

Determine if vCenter Server is reporting the host as not responding. If so, there is a networking problem, an ESXi host agent failure, or a total cluster failure. After the condition is resolved, vSphere HA should work correctly. If not, reconfigure vSphere HA on the host. Similarly, if vCenter Server reports the hosts are responding but a host's state is Agent Unreachable, reconfigure vSphere HA on that host.

vSphere HA Agent is in the Uninitialized State

The vSphere HA agent on a host is in the Uninitialized state for a minute or more. User intervention might be required to resolve this situation.

Problem

vSphere HA reports that an agent is in the Uninitialized state when the agent for the host is unable to enter the run state and become the primary host or to connect to the primary host. Consequently, vSphere HA is not able to monitor the virtual machines on the host and might not restart them after a failure.

Cause

A vSphere HA agent can be in the Uninitialized state for one or more reasons. This condition most often indicates that the host does not have access to any datastores. Less frequently, this condition indicates that the host does not have access to its local datastore on which vSphere HA caches state information, the agent on the host is inaccessible, or the vSphere HA agent is unable to open required firewall ports. It is also possible that the ESXi host agent has stopped.

Solution

Search the list of the host's events for recent occurrences of the event `vSphere HA Agent for the host has an error`. This event indicates the reason for the host being in the uninitialized state. If the condition exists because of a datastore problem, resolve whatever is preventing the host from accessing the affected datastores. If the ESXi host agent has stopped, you must restart it. After the problem has been resolved, if the agent does not return to an operational state, reconfigure vSphere HA on the host.

Note If the condition exists because of a firewall problem, check if there is another service on the host that is using port 8182. If so, shut down that service, and reconfigure vSphere HA.

vSphere HA Agent is in the Initialization Error State

The vSphere HA agent on a host is in the Initialization Error state for a minute or more. User intervention is required to resolve this situation.

Problem

vSphere HA reports that an agent is in the Initialization Error state when the last attempt to configure vSphere HA for the host failed. vSphere HA does not monitor the virtual machines on such a host and might not restart them after a failure.

Cause

This condition most often indicates that vCenter Server was unable to connect to the host while the vSphere HA agent was being installed or configured on the host. This condition might also indicate that the installation and configuration completed, but the agent did not become a primary host or a secondary host within a timeout period. Less frequently, the condition is an indication that there is insufficient disk space on the host's local datastore to install the agent, or that there are insufficient unreserved memory resources on the host for the agent resource pool. Finally, for ESXi 5.x hosts, the configuration fails if a previous installation of another component required a host reboot, but the reboot has not yet occurred.

Solution

When a Configure HA task fails, a reason for the failure is reported.

Reason for Failure	Action
Host communication errors	Resolve any communication problems with the host and retry the configuration operation.
Timeout errors	Possible causes include that the host crashed during the configuration task, the agent failed to start after being installed, or the agent was unable to initialize itself after starting up. Verify that vCenter Server is able to communicate with the host. If so, see vSphere HA Agent Is in the Agent Unreachable State or vSphere HA Agent is in the Uninitialized State for possible solutions.
Lack of resources	Free up approximately 75MB of disk space. If the failure is due to insufficient unreserved memory, free up memory on the host by either relocating virtual machines to another host or reducing their reservations. In either case, retry the vSphere HA configuration task after resolving the problem.
Reboot pending	If an installation for a 5.0 or later host fails because a reboot is pending, reboot the host and retry the vSphere HA configuration task.

vSphere HA Agent is in the Uninitialization Error State

The vSphere HA agent on a host is in the Uninitialization Error state. User intervention is required to resolve this situation.

Problem

vSphere HA reports that an agent is in the Uninitialization Error state when vCenter Server is unable to unconfigure the agent on the host during the Unconfigure HA task. An agent left in this state can interfere with the operation of the cluster. For example, the agent on the host might elect itself as primary host and lock a datastore. Locking a datastore prevents the valid cluster primary host from managing the virtual machines with configuration files on that datastore.

Cause

This condition usually indicates that vCenter Server lost the connection to the host while the agent was being unconfigured.

Solution

Add the host back to vCenter Server (version 5.0 or later). The host can be added as a stand-alone host or added to any cluster.

vSphere HA Agent is in the Host Failed State

The vSphere HA agent on a host is in the Host Failed state. User intervention is required to resolve the situation.

Problem

Usually, such reports indicate that a host has actually failed, but failure reports can sometimes be incorrect. A failed host reduces the available capacity in the cluster and, in the case of an incorrect report, prevents vSphere HA from protecting the virtual machines running on the host.

Cause

This host state is reported when the vSphere HA primary host to which vCenter Server is connected is unable to communicate with the host and with the heartbeat datastores that are in use for the host. Any storage failure that makes the datastores inaccessible to hosts can cause this condition if accompanied by a network failure.

Solution

Check for the noted failure conditions and resolve any that are found.

vSphere HA Agent is in the Network Partitioned State

The vSphere HA agent on a host is in the Network Partitioned state. User intervention might be required to resolve this situation.

Problem

While the virtual machines running on the host continue to be monitored by the primary hosts that are responsible for them, vSphere HA's ability to restart the virtual machines after a failure is affected. First, each primary host has access to a subset of the hosts, so less failover capacity is available to each host. Second, vSphere HA might be unable to restart a FT Secondary VM after a failure. See also *vSphere Availability* troubleshooting.

Cause

A host is reported as partitioned if both of the following conditions are met:

- The vSphere HA primary host to which vCenter Server is connected is unable to communicate with the host by using the management (or VMware vSAN™)network, but is able to communicate with that host by using the heartbeat datastores that have been selected for it.

- The host is not isolated.

A network partition can occur for a number of reasons including incorrect VLAN tagging, the failure of a physical NIC or switch, configuring a cluster with some hosts that use only IPv4 and others that use only IPv6, or the management networks for some hosts were moved to a different virtual switch without first putting the host into maintenance mode.

Solution

Resolve the networking problem that prevents the hosts from communicating by using the management networks.

vSphere HA Agent is in the Network Isolated State

The vSphere HA agent on a host is in the Network Isolated state. User intervention is required to resolve this situation.

Problem

When a host is in the Network Isolated state, there are two things to consider -- the isolated host and the vSphere HA agent that holds the primary role.

■ On the isolated host, the vSphere HA agent applies the configured isolation response to the running VMs, determining if they should be shut down or powered off. It does this after checking whether a primary agent is able to take responsibility for each VM (by locking the VM's home datastore.) If not, the agent defers applying the isolation response for the VM and rechecks the datastore state after a short delay.

■ If the vSphere HA primary agent can access one or more of the datastores, it monitors the VMs that were running on the host when it became isolated and attempts to restart any that were powered off or shut down.

Cause

A host is network isolated if both of the following conditions are met:

■ Isolation addresses have been configured and the host is unable to ping them.

■ The vSphere HA agent on the host is unable to access any of the agents running on the other cluster hosts.

Note If your vSphere HA cluster has vSAN enabled, a host is determined to be isolated if it cannot communicate with the other vSphere HA agents in the cluster and cannot reach the configured isolation addresses. Although the vSphere HA agents use the vSAN network for inter-agent communication, the default isolation address is still the gateway of the host. Hence, in the default configuration, both networks must fail for a host be declared isolated.

Solution

Resolve the networking problem that is preventing the host from pinging its isolation addresses and communicating with other hosts.

Configuration of vSphere HA on Hosts Times Out

The configuration of a vSphere HA cluster might time out on some of the hosts added to it.

Problem

When you enable vSphere HA on an existing cluster with a large number of hosts and virtual machines, the setup of vSphere HA on some of the hosts might fail.

Cause

This failure is the result of a time out occurring before the installation of vSphere HA on the host(s) completes.

Solution

Set the vCenter Server advanced option config.vpxd.das.electionWaitTimeSec to value=240. Once this change is made, the time outs do not occur.

Authentication Token Manipulation Error

Creating a password that does not meet the authentication requirements of the host causes an error.

Problem

When you create a password on the host, the following fault message appears: `A general system error occurred: passwd: Authentication token manipulation error`.

The following message is included: `Failed to set the password. It is possible that your password does not meet the complexity criteria set by the system.`

Cause

The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, the error appears.

Solution

When you create a password, include a mix of characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters such as an underscore or dash.

Your user password must meet the following length requirements.

- Passwords containing characters from three character classes must be at least eight characters long.

- Passwords containing characters from all four character classes must be at least seven characters long.

Note An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

For more information, see the *vSphere Security* documentation.

Unable to Download VIBs When Using vCenter Server Reverse Proxy

You are unable to download VIBs if vCenter Server is using a custom port for the reverse proxy.

Problem

If you configure vCenter Server reverse proxy to use a custom port, the VIB downloads fail.

Cause

If vCenter Server is using a custom port for the reverse proxy, the custom port is not automatically enabled in the ESXi firewall and the VIB downloads fail.

Solution

1 Open an SSH connection to the host and log in as root.

2 (Optional) List the existing firewall rules.

```
esxcli network firewall ruleset list
```

3 (Optional) Back up the `/etc/vmware/firewall/service.xml` file.

```
cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
```

4 Edit the access permissions of the `service.xml` file to allow writes by running the `chmod` command.

   ▪ To allow writes, run chmod 644 `/etc/vmware/firewall/service.xml`.

   ▪ To toggle the sticky bit flag, run chmod +t `/etc/vmware/firewall/service.xml`.

5 Open the `service.xml` file in a text editor.

6 Add a new rule to the `service.xml` file that enables the custom port for the vCenter Server reverse proxy .

```
<service id='id_value'>
    <id>vcenterrhttpproxy</id>
    <rule id='0000'>
      <direction>outbound</direction>
      <protocol>tcp</protocol>
      <port type='dst'>custom_reverse_proxy_port</port>
    </rule>
    <enabled>true</enabled>
    <required>false</required>
</service>
```

Where *id_value* must be a unique value, for example, if the last listed service in the `service.xml` file has ID 0040, you must enter id number 0041.

7 Revert the access permissions of the `service.xml` file to the default read-only setting.

```
chmod 444 /etc/vmware/firewall/service.xml
```

8 Refresh the firewall rules for the changes to take effect.

```
esxcli network firewall refresh
```

9 (Optional) List the updated rule set to confirm the change.

```
esxcli network firewall ruleset list
```

10 (Optional) If you want the firewall configuration to persist after a reboot of the ESXi host, copy the `service.xml` onto persistent storage and modify the `local.sh` file.

    a   Copy the modified `service.xml` file onto persistent storage, for example `/store/`, or onto a VMFS volume, for example `/vmfs/volumes/volume/`.

```
cp /etc/vmware/firewall/service.xml location_of_xml_file
```

        You can store a VMFS volume in a single location and copy it to multiple hosts.

    b   Add the `service.xml` file information to the `local.sh` file on the host.

```
cp location_of_xml_file /etc/vmware/firewall
esxcli network firewall refresh
```

        Where*location_of_xml_file* is the location to which the file was copied.

Troubleshooting Licensing

The troubleshooting licensing topics provide solutions to problems that you might encounter as a result of an incorrect or incompatible license setup in vSphere.

Troubleshooting Host Licensing

You might encounter different problems that result from an incompatible or incorrect license configuration of ESXi hosts.

Unable to Assign a License to an ESXi Host

Under certain conditions, you might be unable to assign a license to an ESXi host.

Problem

You try to assign a license to an ESXi host, but you cannot perform the operation and you receive an error message.

Cause

You might be unable to assign a license to an ESXi host because of the following reasons:

- The calculated license usage for the host exceeds the license capacity. For example, you have a vSphere license key with capacity for two CPUs. You try to assign the key to a host that has four CPUs. You cannot assign the license, because the required license usage for the host is greater than the license capacity.

- The features on the host do not match the license edition. For example, you might configure hosts with vSphere Distributed Switch and vSphere DRS while in evaluation mode. Later, you try to assign vSphere Standard license to the hosts. This operation fails because the vSphere Standard edition does not include vSphere Distributed Switch and vSphere DRS.

- The host is connected to a vCenter Server system that is assigned a license that restricts the edition of the license that you want to assign.

Solution

- Assign a license with larger capacity.

- Upgrade the license edition to match the resources and features on the host, or disable the features that do not match the license edition.

- Assign a vSphere license whose edition is compatible with the license edition of vCenter Server.

ESXi Host Disconnects from vCenter Server

An ESXi host might disconnect from vCenter Server or all ESXi hosts might disconnect from vCenter Server at the same time.

Problem

An ESXi host disconnects from vCenter Server when the host evaluation period or license expires. All ESXi hosts disconnect from vCenter Server when the evaluation period or the license of vCenter Server expire. You receive a licensing-related error message both when a single host disconnects and when all hosts disconnect. You cannot add hosts to the vCenter Server inventory. The hosts and the virtual machines on the hosts continue to run.

Cause

- The 60-day evaluation period of the host has expired or the host license has expired.

- The 60-day evaluation period of vCenter Server is expired or the vCenter Server license is expired.

Solution

- Assign a vSphere license to the ESXi host and try to reconnect it to vCenter Server.

- Assign a vCenter Server license to the vCenter Server system.

Unable to Power On a Virtual Machine

You try to power on a virtual machine, but the operation is unsuccessful and you receive an error message.

Problem

You cannot power on a virtual machine on an ESXi host.

Cause

You might be unable to power on a virtual machine because of the following reasons.

- The 60-day evaluation period of the host is expired.

- The license of the host is expired.

Solution

Table 16-3. Power on a Virtual Machine

Cause	Solution
The evaluation period of the host is expired	Assign a vSphere license to the ESXi host
The license of the host is expired	Assign a vSphere license to the ESXi host

Unable to Configure or Use a Feature

You cannot use a feature or change its configuration.

Problem

You cannot use or configure a feature and a licensing-related error message appears.

Cause

The ESXi host or the vCenter Server system is assigned a license that does not support the features that you want to configure.

Solution

Check the licensed features on the ESXi host and on the vCenter Server system. Upgrade the edition of the license assigned to the host or vCenter Server if they do not include the features that you try to configure or use.