vCenter Server and Host Management

Update 2
11 APR 2019
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About 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.

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.

1 vSphere Concepts and Features

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

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 and vSphere Web 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 a single Windows or Linux Service and is installed to run automatically. 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.

You can install vCenter Server on a Windows virtual machine or physical server, or deploy the vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy the vCenter Server Appliance on ESXi hosts 5.5 or later, or on vCenter Server instances 5.5 or later.

All prerequisite services for running vCenter Server and the vCenter Server components are bundled in the VMware Platform Services Controller. You can deploy vCenter Server with an embedded or external Platform Services Controller, but you must always install or deploy the Platform Services Controller before installing or deploying vCenter Server. All vCenter Server services and some Platform Services Controller 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, multi-mastered directory service that makes an LDAP directory available on port 11711. 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: ICIM/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.

Client Interfaces for vSphere

You can access vSphere components through the vSphere Client, the vSphere Web 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 alongside the vSphere Web Client. The vSphere Client is the primary interface for connecting to and managing vCenter Server instances. Instructions in this guide reflect the vSphere Client (an HTML5-based GUI). You can also use the instructions to perform the tasks by using the vSphere Web Client (a Flex-based GUI). Tasks for which the workflow differs significantly between the vSphere Client and the vSphere Web Client have duplicate procedures that provide steps according to the respective client interface. The procedures that relate to the vSphere Web Client, contain vSphere Web Client in the title.
vSphere Web Client	The vSphere Web Client is a web application installed on a machine with network access to your vCenter Server installation.
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.

Note In vSphere 6.7 Update 1, almost all of the vSphere Web Client functionality is implemented in the vSphere Client. For an up-to-date list of any remaining unsupported functionality, see Functionality Updates for the vSphere Client.

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

The data center defines the namespace for networks and datastores. The names for these objects must be unique within a data center. You cannot have two datastores with the same name within a single data center, but you can have two datastores with the same name in two different data centers. Virtual machines, templates, and clusters need not be unique within the data center, but must be unique within their folder.

Objects with the same name in two different data centers are not necessarily the same object. Because of this, moving objects between data centers can create unpredictable results. For example, a network named networkA in data_centerA might not be the same network as a network named networkA in data_centerB. Moving a virtual machine connected to networkA from data_centerA to data_centerB results in the virtual machine changing the network it is connected to.

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.

If you enable VMware EVC on a cluster, you can ensure that migrations with vMotion do not fail because of CPU compatibility errors. If you enable vSphere DRS on a cluster, the resources of the hosts in the cluster are merged to allow resource balancing for the hosts in the cluster. If you

	enable vSphere HA on a cluster, the resources of the cluster are managed as a pool of capacity to allow rapid recovery from host hardware failures.
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. Data center folders form a hierarchy directly under the root vCenter Server and allow users to group their data centers. Within each data center is one hierarchy of folders with virtual machines and templates, one with hosts and clusters, one with datastores, and one with networks.
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. All virtual machines that connect to the same port group belong to the same network in the virtual environment, even if they are on different physical servers. 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. If DRS is enabled, vCenter Server provides various options for monitoring the status of the resources and adjusting or suggesting adjustments to the virtual machines using the resources. You can monitor resources and set alarms on them.

Templates	A template is a master 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.

Enhancements to Deploying Plug-ins in the vSphere Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_plugins)

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 Update Manager (VUM)	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 Internet Explorer 11 and later. Mozilla Firefox: 56 and later. Google Chrome: 62 and later.
Mac OS	Mozilla Firefox: 56 and later. Google Chrome: 62 and later.

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

This chapter includes the following topics:

- View Recent Objects
- Configure the vSphere Web Client Timeout Value
- Remove Stored User Data
- Drag Objects
- Export Lists
- Attach File to Service Request
- Keyboard Shortcuts
- Provide Feedback with the vSphere Client

Log In to vCenter Server by Using the vSphere Client

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

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

Procedure

1. Open a Web browser and enter the URL for your vCenter Server instance: `https://vcenter_server_ip_address_or_fqdn`
2. Select **Launch vSphere Client (HTML5)**. To use the vSphere Web Client, select **Launch vSphere Web Client (Flex)**.

   You can instead open a Web browser and enter the URL for the vSphere Client: `https://vcenter_server_ip_address_or_fqdn/ui`. To use the vSphere Web Client, enter the URL: `https://vcenter_server_ip_address_or_fqdn/vsphere-client`.
3. Enter the credentials of a user who has permissions on vCenter Server, and click **Login**.
4. If a warning message about an untrusted SSL certificate appears, select the appropriate action based on your security policy.

Option	Action
Ignore the security warning for this login session only.	Click **Ignore**.
Ignore the security warning for this login session, and install the default certificate so that the warning does not appear again.	Select **Install this certificate and do not display any security warnings for this server** and click **Ignore**. Select this option only if using the default certificate does not present a security problem in your environment.
Cancel and install a signed certificate before proceeding.	Click **Cancel** and ensure that a signed certificate is installed on the vCenter Server system before you attempt to connect again.

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

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

Use the vSphere Client Navigator

You can use the navigator to browse and select objects in the vSphere Client 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 views, the navigator presents a graph-based view of the inventory. You can navigate from an object to its related objects, regardless of type.

Procedure

1. From the vSphere Client Home, click **Global Inventory Lists**.
2. Under **Global Inventory Lists**, click one of the object categories to view objects of that type.

   For example, click **Hosts** to view hosts in the vSphere Client inventory.
3. Click an object in the list once to display information about the object in the center pane of the vSphere Client.
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, vApps, datastores, standard networks, distributed switches, and distributed port groups associated with this host.
5. To access additional information and actions, click one of the tabs in the center pane.

Option	Description
Getting Started	View introductory information and access basic actions.
Summary	View basic status and configuration for an object.
Monitor	View alarms, performance data, resource allocation, events, and other status information for an object.
Configure	Configure settings, alarm definitions, tags, and permissions.
Permissions	View, add, change, and delete permissions. This tab is only available for logged in users with administration privileges.
Related Objects tabs	Tabs with lists of 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**.

Customize the User Interface

You can customize the look and feel of vSphere Client to improve your experience while you perform your tasks.

After you customize the user interface, vSphere Client saves the individual user interface customization.

- Rearrange the Components of the User Interface

  You can rearrange the panes in the vSphere Web Client user interface. You can move the panes and Navigator sidebar around the content area to enhance your personal experience by customizing the vSphere Web Client user interface. You change the interface at any time.

- Customize the User Interface by Using the Layout Settings Menu

  You can customize the user interface of vSphere Web Client by choosing to hide or display different panes.

- Disable the vSphere Web Client Customizable User Interface Feature

  You can disable the vSphere Web Client customizable user interface feature by changing the `webclient.properties` file of vCenter Server or vCenter Server Appliance.

- Disable the Related Objects Tabs

  You can disable the related object tabs by changing the `webclient.properties` file.

Rearrange the Components of the User Interface

You can rearrange the panes in the vSphere Web Client user interface. You can move the panes and Navigator sidebar around the content area to enhance your personal experience by customizing the vSphere Web Client user interface. You change the interface at any time.

Procedure

1. In a Web browser, log in to vSphere Web Client.
2. Drag the pane you want to move to an appropriate place.

   While you drag the pane, you see two types of arrows. Single arrows move as you drag from one part of the UI to another. Both single and double arrows indicate the target position of the pane you want to move.

Customize the User Interface by Using the Layout Settings Menu

You can customize the user interface of vSphere Web Client by choosing to hide or display different panes.

Procedure

1. In a Web browser, log in to vSphere Web Client.
2. Click the user name at the top of the vSphere Web Client window and select **Layout Settings**.
3. In the **Layout Settings** window, select the panes that you want the UI to display.

4 Click **OK** to save the changes.

Disable the vSphere Web Client Customizable User Interface Feature

You can disable the vSphere Web Client customizable user interface feature by changing the `webclient.properties` file of vCenter Server or vCenter Server Appliance.

Procedure

1 Connect to the vCenter Server or vCenter Server Appliance by using any remote console, and optionally use SSH.

2 Navigate to the `webclient.properties` file and open it in a text editor.

Option	Description
vCenter Server	*installation_directory*\VMware\CIS\cfg\vsphere-client\webclient.properties
vCenter Server Appliance	/etc/vmware/vsphere-client/webclient.properties

3 On a new line, enter **`docking.disabled=true`** and save the file.

Disable the Related Objects Tabs

You can disable the related object tabs by changing the `webclient.properties` file.

Procedure

1 Connect to the vCenter Server or vCenter Server Appliance by using any remote console, and optionally use SSH.

2 Navigate to the `/etc/vmware/vsphere-client/webclient.properties` file and open it in a text editor.

3 Edit the file to include the line `show.relations.in.categorized.tabs=false`.

If the line is present but commented out, remove the comment indicator.

4 Restart the vSphere Web Client service.

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 Plug-ins**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. From the home sidebar menu, click **Administration > Solutions > Client Plug-Ins**.

   The Client Plug-In 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) To enable or disable a client plug-in, select the radio button next to the plug-in and click **Enable** or **Disable**.

Install the VMware Enhanced Authentication Plug-in

The VMware Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality.

In the vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaced the Client Integration Plug-in from vSphere 6.0 releases and earlier. The Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality. These are the only two features carried over from the previous Client Integration Plug-in. The Enhanced Authentication Plug-in can function seamlessly if you already have the Client Integration Plug-in installed on your system from vSphere 6.0 or earlier. There are no conflicts if both plug-ins are installed.

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

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

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

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

Procedure

1. Open a Web browser and type the URL for the vSphere 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.

Pause and Resume a Task in Progress in the vSphere Web Client

You can pause many tasks in the vSphere Web Client and later resume them from the Work in Progress pane.

Procedure

1 In a dialog box or wizard, click the minimize button.

   The task is paused and minimized to the Work in Progress pane. Any changes that you have made in the dialog box or wizard are saved, but not yet applied to the object you are working with.

2 When you are ready to resume the task, click it in the Work in Progress pane.

   The dialog box or wizard opens and you can resume the task from where you left off.

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 vSphere Client, you can search the inventory for objects that match specified criteria. You can search the inventories of all vCenter Server systems connected to the same Platform Services Controller or to Platform Services Controllers.

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.

- Perform a Simple Search

  A simple search checks all types of objects for a specified search term within the object name.

- Perform an Advanced Search

  You can conduct an advanced search in the vSphere Web Client to search for managed objects that meet multiple criteria.

- Save, Run, Rename, and Delete a Search

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

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. Type 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 display an item in the inventory, click that item in the search results.
3. (Optional) To see more search results or more details about the search results, click **All Results**.
   a. (Optional) To see additional information about the object, select an object in the results table.
   b. (Optional) To display that item in the inventory, double-click any item in the search results.

   The search results are listed in a table. If differing types of objects are found, the table contains tabs for each type of object. For example, if a search finds hosts and virtual machines, the following tabs appear: **Hosts**, showing only host results and **Virtual Machines**, showing only virtual machine results.

Perform a Simple Search

A simple search checks all types of objects for a specified search term within the object name.

Procedure

1. From the vSphere Client Home screen sidebar menu, click **New Search**
2. Type the search term in the search box and press Enter.

   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 are listed in a table. If differing types of objects are found, the table contains tabs for each type of object. For example, if a search finds hosts and virtual machines, the following tabs appear: **Hosts**, showing only host results and **Virtual Machines**, showing only virtual machine results.
3. (Optional) To see additional information about the object, select the object in the results table.
4. (Optional) To display an item in the inventory, double-click that item in the search results.

Perform an Advanced Search

You can conduct an advanced search in the vSphere Web Client to search for managed objects that meet multiple criteria.

For example, you can use specific strings to search for virtual machines residing on a particular host.

Procedure

1. From the vSphere Web Client Home, click **New Search** and then click **Advanced Search**.
2. Select the type of object to search for from the **Search for** drop-down menu.
3. Select how to combine the search criteria.

Option	Description
any	The search returns results that match any of the specified criteria.
all	The search returns only results that match all the specified criteria.

4. Select a property to search for from the drop-down menu.

   The properties available depend on the type of object you are searching for.
5. Select the relationship between the search term and the property from the drop-down menu.

   The options available in this step depend on the property selected in the previous step. For example, if you select a **Name** property, the options available are **contains**, **is**, and **is not**.
6. Type or select the search term.
7. (Optional) To add additional search criteria, click **Add new criteria** and repeat step 4 to step 6.
8. (Optional) To add an additional search, click **Add another object type** and repeat step 2 to step 7.
9. Click **Search**.

   Search results are displayed in the details pane and in the navigator.

10 (Optional) To see item details without leaving the context of the search, click on the item in the navigator.

11 (Optional) To display an item in the inventory, double-click on the item in the details pane.

Save, Run, Rename, and Delete a Search

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

Procedure

1 In the vSphere Client, enter a query for either a simple or advanced search.

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

3 Enter a name for the search query. Names must be lowercase with no spaces. Click **Save**

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

4 To run a saved search, go to the quick search field and click the saved search icon. Select the search query you want to run.

5 To rename a saved search, go to the search results page and click the **Actions** dropdown. Select **Rename**.

6 To create a duplicate saved search query, go to the search results page and click the **Actions** dropdown. Select **Save As**.

7 To delete a saved search query, go to the search results page and click the **Actions** dropdown. Select **Delete**.

Use Quick Filters

You can use quick filters to find an object or a set of objects in your vSphere Web Client inventory that fit certain criteria.

Quick filters are available in the list views, which appear in the **Objects** tab of an inventory list and in search results.

For example, you can use the quick filter options for virtual machines to find all virtual machines in your vSphere inventory that are powered on but do not have VMware Tools running.

Procedure

1 From the vSphere Web Client, open a list view.

You can access list views of objects from the **Inventory Lists** and the search results.

2 Click **Show and hide quick filters** ( ) next to the filter box, and select from the available options.

A list of inventory objects that meet your selection criteria is displayed.

What to do next

To clear the filtered list of vSphere inventory objects, deselect the filter criteria or click **Clear** next to the filter group name.

Quick Filters Available for vSphere Objects

Various types of quick filters are available for the vSphere objects in your inventory. No quick filters are available for linked vCenter Server systems, host profiles, and extensions.

Tags are a quick filter option available for all types of vSphere objects, except for linked vCenter Server systems, host profiles, and extensions. You can filter data centers, vApps, and resource pools only by using the tags that are assigned to them. For datastores, clusters, hosts, virtual machines, and VM templates, you can use a number of different quick filters.

Quick Filters for Datastores

You can filter datastores by the following criteria:

- Tags
- Type
- Belongs to Datastore Cluster
- Accessibility
- Maintenance Mode
- Drive Type
- % Free Space
- Storage I/O Control

Quick Filters for Clusters

You can filter clusters by the following criteria:

- Tags
- vSphere DRS
- vSphere HA
- vSAN

Quick Filters for Hosts

You can filter hosts by the following criteria:

- Tags
- Connection State
- Type
- Maintenance Mode

- Standalone or Clustered
- Power State
- CPUs
- NICs
- ESX/ESXi Version
- vSphere vMotion
- Host Compliance
- HA State
- vSphere Fault Tolerance
- EVC Mode

Quick Filters for Virtual Machines

You can filter virtual machines by the following criteria:

- Tags
- State
- Needs Consolidation
- Blocked by Question
- Encryption
- vSphere FT Role
- Has Snapshot
- VMware Tools Version Status
- VMware Tools Running Status
- EVC Mode
- Guest OS
- Compatibility
- CPUs
- NICs

Quick Filters for VM Templates

You can filter virtual machine templates by the following criteria:

- Tags
- VMware Tools Version Status
- Guest OS

- Compatibility
- CPUs
- NICs

View Recent Objects

You can quickly navigate to the objects that you visited during your vSphere Web Client session. You can switch between objects you last visited without having to search for the objects in the object navigator or in the inventory tree.

In the **Recent Objects** pane, you can see a history of the most recent objects that you visited in your environment. You can see the most recent objects that you visited and the latest objects that you created. The recent objects list is persistent between vSphere Web Client sessions, but the new objects list is not persistent between vSphere Web Client sessions.

Procedure

1 In the **Recent Objects** pane, select the tab that you want to view.

Objects are listed in two tabs depending on whether you visited or created the object.

Tab	Description
Viewed	The last objects that you visited in the vSphere Web Client inventory.
Created	The latest objects that you created in the vSphere Web Client inventory.

2 Click the object that you want to view.

The object displays in the center pane of the vSphere Web Client

You have navigated to the object that you selected in the **Recent Objects** pane.

Configure the vSphere Web Client Timeout Value

By default, vSphere Web Client sessions close after 120 minutes of idle time, requiring the user to log in again to resume using the client. You can change the timeout value by editing the `webclient.properties` file.

Procedure

1 On the computer where the vSphere Web Client is installed, locate the `webclient.properties` file.

The location of this file depends on the operating system on which the vSphere Web Client is installed.

Operating System	File path
Windows 2008	`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client`
vCenter Server Appliance	`/etc/vmware/vsphere-client/`

2 Edit the file to include the line `session.timeout = value` where value is the timeout value in minutes. Uncomment the line, if necessary.

   To set the client to never timeout, specify a negative or 0 value for the timeout.

   For example, to set the timeout value to 60 minutes, include the line `session.timeout = 60`.

3 Restart the vSphere Web Client service.

   - On Windows operating systems, restart the VMware vSphere Web Client service.
   - On the vCenter Server Appliance, restart the vSphere-client service.

Remove Stored User Data

The vSphere Web Client stores user data including saved searches, Work In Progress items, and Getting Started Pages preferences. You can remove this stored data to reset these items to the initial defaults and remove stored data that you no longer need.

You can remove data only for the currently logged-in user. Data stored by other users is not affected.

Procedure

1 In the vSphere Web Client, click the name of the currently logged-in user and select **Remove Stored Data**.

2 Select the data to remove.

Option	Description
"Work in progress" items	Removes all current Work In Progress items for this user.
Getting Started Pages preferences	Removes all Getting Started pages preferences for this user. All Getting Started pages are displayed in the vSphere Web Client.
Saved Searches	Removes all Saved Searches for this user.
User preferences for Update Manager views	Removes all Update Manager view preferences for this user.
User preferences for columns in list views	Removes all list view column preferences for this user.

3 Click **Clear Selected Data**

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 In the vSphere Client inventory tree or in a list view, select an inventory object group.

You can drag objects within the vSphere Client inventory tree, or within a list view to the inventory tree.

You can access list views from the **Global Inventory Lists** and search results.

2 Drag an object 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 panel.

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

The object is moved to the destination object you selected.

Export Lists

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

Procedure

1 From the vSphere Client, open a list view for an object type, for example, Virtual Machines or Hosts

You can access list views of objects from the **Global Inventory Lists** and the search results.

2 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.

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

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

5 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**.

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 Web Client.

Inventory Keyboard Shortcuts

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

Table 2-3. Inventory Keyboard Shortcuts

Keyboard Combination	Action
Ctrl+Alt+s	Quick search
Ctrl+Alt+Home or Ctrl+Alt+1	Home
Ctrl+Alt+2	Hosts and Clusters
Ctrl+Alt+3	VMs and Templates
Ctrl+Alt+4	Storage
Ctrl+Alt+5	Networking
Ctrl+Alt+6	Content Libraries
Ctrl+Alt+7	Global Inventory Lists

Create a Scheduled Task with a Keyboard Shortcut

You can use a keyboard shortcut to create a scheduled task.

For more information about how to schedule tasks, see Schedule Tasks.

Procedure

1 Select the **Actions** menu, point to an action, and press Ctrl.

The clock icon ( ) appears next to the action that you can schedule.

2 Select the action and configure the scheduling options.

3 Navigate to the object in the inventory.

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**.

Configuring vCenter Server

3

You can configure vCenter Server from the vSphere Client and from the vSphere Web Client.

What you can do depends on your deployment.

On-premises vCenter Server	You can change many of the vCenter Server settings, including licensing, statistics collection, logging, and more.
vCenter Server in VMware Cloud on AWS	VMware preconfigures vCenter Server instances when you create an SDDC. You can view configuration settings and advanced settings, and you can set a Message of the Day.

This chapter includes the following topics:

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 My VMware, 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 or the vSphere Web Client runs.

Procedure

1. Navigate to the vCenter Server system.
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**.

   - In the vSphere Web 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 **Create New License** () icon. b In the **New Licenses** dialog box, type or copy and paste a license key and click **Next**. c On the **Edit license names** page, enter a name for the new license and click **Next**. d Click **Finish**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

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

Configuring Statistics Settings

To set up how statistical data is recorded, you configure collection intervals for statistics. You can access the stored statistical information through command-line monitoring utilities or by viewing performance charts in the vSphere Client.

Configure Statistics Collection Intervals in the vSphere Client

Statistic collection intervals determine the frequency at which statistic queries occur, the length of time statistical data is stored in the database, and the type of statistical data that is collected. You can view the collected statistics through the performance charts in the vSphere Client or through command-line monitoring utilities.

Note Not all interval attributes are configurable.

Prerequisites

Required privilege: **Performance.ModifyIntervals**

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. To enable or disable a statistics interval, check the box for that interval.
6. To change a statistics interval attribute value, select a value from the drop-down menu.
   a. In **Interval Duration**, select the time interval in which statistics data is collected.
   b. In **Save For**, select for how long the archived statistics are kept in the database.
   c. In **Statistics Level**, select a new level for collecting statistics.

      The lower the level is, the fewer number of statistic counters are used. Level 4 uses all statistics counters. Use it only for debugging purposes.

      The statistics level must be less than or equal to the statistics level that is set for the preceding statistics interval. This requirement is a vCenter Server dependency.

7 (Optional) In Database Size, estimate the effect of the statistics settings on the database.

   a Enter the number of **Physical Hosts**.

   b Enter the number of **Virtual Machines**.

      The estimated space required and number of database rows required are calculated and displayed.

   c If necessary, make changes to your statistics collection settings.

8 Click **Save**.

Example: Relationships Between the Default Settings for Statistics Intervals

- Samples that are collected every 5 minutes are stored for 1 day.
- Samples that are collected every 30 minutes are stored for 1 week.
- Samples that are collected every 2 hours are stored for 1 month.
- Samples that are collected on 1 day are stored for 1 year.

For all statistics intervals, the default level is 1. It uses the Cluster Services, CPU, Disk, Memory, Network, System, and Virtual Machine Operations counters.

Data Collection Levels

Each collection interval has a default collection level that determines the amount of data gathered and which counters are available for display in the charts. Collection levels are also referred to as statistics levels.

Table 3-1. Statistics Levels

Level	Metrics	Best Practice
Level 1	■ Cluster Services (VMware Distributed Resource Scheduler) – all metrics ■ CPU – cpuentitlement, totalmhz, usage (average), usagemhz ■ Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used ■ Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon) ■ Network – usage (average), IPv6 ■ System – heartbeat, uptime ■ Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required. Level 1 is the default Collection Level for all Collection Intervals.
Level 2	■ Level 1 metrics ■ CPU – idle, reservedCapacity ■ Disk – All metrics, excluding numberRead and numberWrite. ■ Memory – All metrics, excluding memUsed and maximum and minimum rollup values. ■ Virtual Machine Operations – All metrics	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.

Level	Metrics	Best Practice
Level 3	■ Level 1 and Level 2 metrics ■ Metrics for all counters, excluding minimum and maximum rollup values. ■ Device metrics	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 3 for the shortest time period (Day or Week collection interval).
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 4 for the shortest amount of time.

Note When you increase the collection level, the storage and system requirements might change. You might need to allocate more system resources to avoid a decrease in the performance.

Configure Runtime Settings for vCenter Server

You can change the vCenter Server ID, managed address, and name. You might need to make changes if you run multiple vCenter Server systems in the same environment.

Prerequisites

Required privilege: **Global.Settings**

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. In the Edit vCenter Server Settings dialog box, select **Runtime Settings**.
6. In **vCenter Server unique ID**, enter a unique ID.

   You can change this value to a number from 0 through 63 to identify each vCenter Server system running in a common environment. By default, an ID value is generated randomly.
7. In **vCenter Server managed address**, enter the vCenter Server system address.

   The address can be IPv4, IPv6, a fully qualified domain name, an IP address, or another address format.

8 In **vCenter Server name**, enter the name of the vCenter Server system.

   If you change the DNS name of the vCenter Server, you can use this text box to modify the vCenter Server name to match.

9 Click **Save**.

What to do next

If you made changes to the vCenter Server system unique ID, you must restart the vCenter Server system for these changes to take effect.

Configure User Directory Settings

You can configure some of the ways vCenter Server interacts with the user directory server that is configured as an identity source.

For vCenter Server versions before vCenter Server 5.0, these settings apply to an Active Directory associated with vCenter Server. For vCenter Server 5.0 and later, these settings apply to vCenter Single Sign-On identity sources.

Prerequisites

Required privilege: **Global.Settings**

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 **User directory**.

6 In **User directory timeout**, type the timeout interval in seconds for connecting to the directory server.

7 Enable the **Query Limit** box to set a query limit size.

8 In **Query Limit Size**, enter the number of users and groups for which you can associate permissions on the child inventory objects of the vCenter Server system.

   You can associate permissions with users and groups from the Add Permissions dialog box that displays when you click **Add permissions** in **Manage > Permissions** for a vSphere inventory object.

9 Enable the **Validation** box to have vCenter Server periodically check its known users and groups against the user directory server.

10 In **Validation Period**, enter the number of minutes between instances of synchronization.

11 Click **Save**.

Configure Mail Sender Settings

You must configure the email address of the sender account if you want to enable vCenter Server operations, such as sending email notifications as alarm actions.

Prerequisites

Required privilege: **Global.Settings**

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 **Mail**.
6. In **Mail server**, type the SMTP server information.

   The SMTP server is the DNS name or IP address of the SMTP gateway to use for sending email messages.
7. In **Mail sender**, type the sender account information.

   The sender account is the email address of the sender.

   Note You must type the full email address, including the domain name.

   For example, *mail_server@example.com*.
8. Click **Save**.

What to do next

To test the mail settings, create an alarm that can be triggered by a user action, such as by powering off a virtual machine, and verify that you receive an email when the alarm is triggered.

Configure SNMP Settings

You can configure up to four receivers to receive SNMP traps from vCenter Server. For each receiver, specify a host name, port, and community.

Prerequisites

Required privilege: **Global.Settings**

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 **SNMP receivers**.

6 Select the **Enable receiver 1** box.

7 In **Primary Receiver URL**, enter the host name or IP address of the SNMP receiver.

8 In **Receiver port**, enter the port number of the receiver.

The port number must be a value between 1 and 65535.

9 In **Community string**, enter the community identifier.

10 To send alarms to multiple receivers, select the additional **Enable receiver** boxes and enter the host name, port number, and community identifier for those receivers.

11 Click **Save**.

View Port Settings

You can view the ports used by the Web service to communicate with other applications. You cannot configure these port settings.

The Web service is installed as part of the VMware vCenter Server installation. The Web service is a required component for third-party applications that use the VMware SDK application programming interface (API). For information about installing the Web service, see the *vCenter Server Installation and Setup* documentation.

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 **Ports**.

The ports used by the Web service are displayed.

6 Click **Save**.

Configure Timeout Settings

You can configure the timeout intervals for vCenter Server operations. These intervals specify the amount of time after which the vSphere Client times out.

Prerequisites

Required privilege: **Global.Settings**

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 **Timeout settings**.
6. In **Normal**, type the timeout interval in seconds for normal operations.

   Do not set the value to zero (0).
7. In **Long**, enter the timeout interval in minutes for long operations.

   Do not set the value to zero (0).
8. Click **Save**.
9. Restart the vCenter Server system for the changes to take effect.

Configure Logging Options

You can configure the amount of detail that vCenter Server collects in log files.

Prerequisites

Required privilege: **Global.Settings**

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 **Logging settings**.
6. Select the logging options.

Option	Description
None (Disable logging)	Turns off logging
Error (Errors only)	Displays only error log entries
Warning (Errors and warnings)	Displays warning and error log entries
Info (Normal logging)	Displays information, error, and warning log entries
Verbose (Verbose)	Displays information, error, warning, and verbose log entries
Trivia (Extended verbose)	Displays information, error, warning, verbose, and trivia log entries

7 Click **Save**.

Changes to the logging settings take effect immediately. You do not need to restart the vCenter Server system.

Configure Database Settings

You can configure the maximum number of database connections that can occur simultaneously. To limit the growth of the vCenter Server database and save storage space, you can configure the database to discard information about tasks or events periodically.

Note Do not use the database retention options if you want to keep a complete history of tasks and events for your vCenter Server.

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 **Database**.

6 In **Maximum connections**, type a number.

Increase this number if your vCenter Server system performs many operations frequently and performance is critical. Decrease this number if the database is shared and connections to the database are costly. Do not change this value unless one of these issues pertains to your system.

7 To have vCenter Server periodically delete the retained tasks, select the **Enabled** box next to Task cleanup.

8 (Optional) In **Task retention (days)**, type a value in days.

Information about tasks that are performed on this vCenter Server system is discarded after the specified number of days.

9 To have vCenter Server periodically clean up the retained events, select the **Enabled** box next to Event cleanup.

10 (Optional) In **Event retention (days)**, type a value in days.

Information about events for this vCenter Server system is discarded after the specified number of days.

11 (Optional) To monitor vCenter Server database consumption and disk partition, open the vCenter Server Appliance Management Interface.

12 Click **Save**.

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**.

Configure Advanced Settings

In **Advanced Settings**, you can modify the vCenter Server configuration file, `vpxd.cfg`.

You can use **Advanced Settings** to add entries to the `vpxd.cfg` file, but not to edit or delete them. VMware recommends that you change these settings only when instructed to do so by VMware technical support or when you are following specific instructions in VMware documentation.

Prerequisites

Required privilege: **Global.Settings**

Procedure

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Select **Advanced Settings**.
4. Click **Edit Settings**.
5. In the **Name** field, type a name for the setting. Names must start with 'config.' For example: **`config.log`**.
6. In the **Value** field, type the value for the specified setting.
7. Click **Add**.
8. Click **Save**.

Newly added advanced settings have `config.` appended to the setting keys in the `vpxd.cfg` file. For example:

```
config.example.setting = exampleValue
```

What to do next

Many advanced settings changes require you to restart the vCenter Server system. Consult VMware technical support to determine if your changes require a restart.

Send a Message to Other Logged In Users

Administrators can send messages to users who are currently logged in to a vCenter Server system. The message might announce maintenance or ask users to log out temporarily.

Procedure

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Click **Configure**.
3. Select **Settings > Message of the Day** and click **Edit**.
4. Enter a message and click **OK**.

The message appears at the top of the vSphere Client in each active user session.

Edit the Settings of Services

The vSphere Web Client lists all manageable services running on vCenter Server. You can edit the settings for some of the services.

The vSphere Web Client displays information about all manageable services running in vCenter Server and the vCenter Server Appliance. A list of the default services is available for each vCenter Server instance.

Note Starting with vSphere 6.5, all vCenter Server services and some Platform Services Controller services run as child processes of the VMware Service Lifecycle Manager service.

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 as administrator@*your_domain_name* to the vCenter Server instance by using the vSphere Web Client.
2. On the vSphere Web Client Home page, under **Administration**, click **System Configuration**.
3. Under **System Configuration**, click **Nodes** and select a node from the list.
4. Click the **Related Objects** tab.

   You see the list of services running in the node you selected. Editable settings are not available for all manageable services.
5. Right-click a service from the list and click **Settings**.

   Editable settings are not available for all manageable services.
6. On the **Manage** tab, click the **Edit** button.
7. Edit the service configuration properties.
8. Click **OK** to save the settings.
9. (Optional) From the **Actions** menu, select **Restart**.

   Restart the service only if a restart is required to apply the configuration changes.

Start, Stop, and Restart Services

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

Note Starting with vSphere 6.5, all vCenter Server services and some Platform Services Controller services run as child processes of the VMware Service Lifecycle Manager service.

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 by using the vSphere Web Client.
2. On the vSphere Web Client Home page, click **System Configuration**.
3. Under System Configuration click **Services**.
4. From the Services list select a manageable service.
5. From the **Actions** menu select an operation name.
   - **Restart**
   - **Start**
   - **Stop**

   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.

Configuring Services in the vSphere Web Client

You can monitor and manage services by using the vSphere Web Client. You can change the settings of only a few services.

There are slight differences between the services available for a vCenter Server instance that runs on a Windows system and those available for vCenter Server Appliance on Linux.

Note Only the default values of the service properties have undergone all product testing cycles. Avoid the usage of nondefault values without guidance from VMware.

Note Starting with vSphere 6.5, all vCenter Server services and some Platform Services Controller services run as child processes of the VMware Service Lifecycle Manager service.

Services that You Can Configure in vCenter Server Appliance

You can use vSphere Web Client to configure the following services in vCenter Server Appliance:

Service	Description
Auto Deploy	Lets you perform stateless ESXi caching. See Auto Deploy Service.
Content Library Service	Manages OVF templates, ISO images, and scripts for vSphere administrators. See Content Library Service.
Transfer Service	Provides support for moving content, such as VM templates, scripts, and ISO images across sites and vCenter Server instances. **Note** Runs as a child service of the Content Library Service. For a list of settings you can configure for this service, see Transfer Service Properties.

Service	Description
Ovf Service	Supports the provisioning of OVF based virtual machines. **Note** Runs as a child service of the Content Library Service. For a list of settings you can configure for this service, see VMware Open Virtualization Format Service .
ImageBuilder Service	Lets you manage and customize Image Profiles. See Image Builder Service.
VMware Performance Charts Service	Collects and processes statistical performance data for managed entities into reports in image format that it provides to the vSphere Web Client. See VMware Performance Charts Service.
VMware vSphere Authentication Proxy	Provides support for joining unattended ESXi hosts to an Active Directory domain by using an account with delegated privileges, enhancing security for PXE-booted hosts and hosts that are provisioned using Auto Deploy. See VMware vSphere Authentication Proxy.
VMware vSphere ESXi Dump Collector Service	Collects core dumps from remote hosts. See VMware vSphere ESXi Dump Collector.
VMware vSphere Update Manager Extension	Provides centralized, automated patch and version management for ESXi hosts, virtual machines, and virtual appliances. See VMware vSphere Update Manager.
vAPI Endpoint	Provides a single point of access to vAPI services. For a list of general settings that you can configure for this service, see vAPI Endpoint.

Services that you can configure in vCenter Server

You can configure the following services on a vCenter Server instance that runs on a Windows machine:

Service Name	Description
Auto Deploy	Lets you perform stateless ESXi caching. See Auto Deploy Service.
Content Library Service	Manages OVF templates, ISO images, and scripts for vSphere administrators. See Content Library Service.
Transfer Service	Provides support for moving content, such as VM templates, scripts, and ISO images across sites and vCenter Server instances. **Note** Runs as a child service of the Content Library Service. For a list of settings you can configure for this service, see Transfer Service Properties.
Ovf Service	Supports the provisioning of OVF based virtual machines. **Note** Runs as a child service of the Content Library Service. For a list of settings you can configure for this service, see VMware Open Virtualization Format Service .
ImageBuilder Service	Lets you manage and customize Image Profiles.
VMware Performance Charts Service	Collects and processes statistical performance data for managed entities into reports in image format that it provides to the vSphere Web Client. See VMware Performance Charts Service.
VMware vSphere Authentication Proxy	Provides support for joining unattended ESXi hosts to an Active Directory domain by using an account with delegated privileges, enhancing security for PXE-booted hosts and hosts that are provisioned using Auto Deploy.

Service Name	Description
VMware vSphere ESXi Dump Collector Service	Collects core dumps from remote hosts. See VMware vSphere ESXi Dump Collector.
vAPI Endpoint	Provides a single point of access to vAPI services. For a list of general settings that you can configure for this service, see vAPI Endpoint.

Auto Deploy Service

vSphere Auto Deploy uses the Auto Deploy Service for stateless ESXi caching. You can change the default configuration properties of the Auto Deploy service.

Auto Deploy and the Auto Deploy Service are installed as part of the vCenter Server installation.

Property	Default Value	Description
cachesize_GB	2	Auto Deploy cache size in gigabytes. The maximum size of an ESXi image or host profile uploads.
loglevel	INFO	The default Auto Deploy log level. Includes information, warnings, errors, and fatal errors.
managementport	6502	Auto Deploy management port. The port on which interfaces that create rules for Auto Deploy, such as vSphere PowerCLI, communicate.
serviceport	6501	Auto Deploy service port. Auto Deploy uses this port to power on ESXi hosts.

Content Library Service

The Content Library service provides simple and effective management of OVF templates, ISO images, and scripts for vSphere administrators. The Content Library service lets you synchronize content across vCenter Server instances.

Property	Default Value	Description
Download Session Expiration Timeout (milliseconds)	300000	Download session expiry timeout in milliseconds. The download session indicates the time for downloading content from a content library item.
Force HTTP for Library Sync	false	Forces data transfers to go through HTTP instead of HTTPS, regardless of the subscription URL protocol. The usage of HTTP improves the speed of file transfer but might cause problems if content libraries contain sensitive information.
Garbage Collect Interval (minutes)	60	Interval in minutes for Content library garbage collection. Garbage collection cleans content library data and files that are no longer used.

Property	Default Value	Description
Garbage Collect Max Retries	5	Number of attempts to clean the content library after the deletion of files fails. Garbage collection cleans content library data and files that are no longer used.
Garbage Collection Start Hour	22	The time of the day when the content library garbage collection starts.
Garbage Collection Stop Hour	8	The time of the day when the content library garbage collection stops.
Library Auto Sync Enabled	true	Enables automatic synchronization of subscribed content libraries.
Library Auto Sync Refresh Interval (minutes)	240	Interval between two consequent automatic synchronizations of the subscribed content library. Measured in minutes.
Library Auto Sync Setting Refresh Interval (seconds)	600	Refresh interval for the automatic synchronization settings of the subscribed library. Measured in seconds. If you change the refresh interval, you must restart vCenter Server
Library Auto Sync Start Hour	20	The time of the day when the automatic synchronization of a subscribed content library starts.
Library Auto Sync Stop Hour	7	The time of the day when the automatic synchronization of a subscribed content library stops. Automatic synchronization stops until the start hour.
Library File Preparation No-Progress Timeout (minutes)	30	Timeout for file preparation of the subscribed content library, measured in minutes.
Library HTTP Connection Timeout (milliseconds)	500000	The HTTP connection timeout for subscribed library, measured in milliseconds.
Library HTTP Socket Connection Timeout (milliseconds)	300000	Subscribed library HTTP connection socket timeout, measured in milliseconds.
Library Maximum Concurrent Sync Items	5	Maximum number of concurrently synchronizing library items for each subscribed library.
Update Session Expiration Timeout (milliseconds)	300000	Update session expiration timeout, measured in milliseconds. Update session is for uploading content to library item.

Note You must log in as a user with an Administrator or a Content library administrator role to change the settings of the Content Library service.

Transfer Service Properties

The Transfer Service lets you move content, such as VM templates, scripts, and ISO images across sites and vCenter Server instances. The Transfer Service has a set of configurable properties that you can change to meet the needs of your virtual environment.

Property	Default Value	Description
Forced Flush to Output Interval	45	Interval between forced flushes to output stream, measured in seconds.
Http Client Buffer Size	262144	Buffer size of the HTTP client input stream during transfers, measured in bytes.
Http Client Socket Timeout	180	Socket timeout of the HTTP client, measured in seconds.
Http Request-handling Timeout	120	Request handling timeout for HTTP transfers, after which service unavailable status is returned to client, measured in seconds.
Http Socket Buffer Size	2048	Buffer size of the HTTP client socket, measured in bytes.
Intermediary I/O Stream Buffer Size	131072	Maximum size of buffer sitting between input and output streams during a transfer, measured in bytes.
Maximum Bandwidth Consumption	0	Bandwidth usage threshold across all transfers, measured in megabits per second Mbps. 0 means unlimited bandwidth.
Maximum Number of Concurrent Priority Transfers	5	Concurrent transfer limit for priority files. If exceeded, transfers are queued. This threadpool is used only to transfer priority objects.
Maximum Number of Concurrent Transfers	20	Concurrent transfer limit. If exceeded, transfers are queued.
NFC Connection Socket Timeout	120	Socket timeout for an NFC connection, measured in seconds. An NFC connection is opened only when interacting with a datastore.
NFC Eager-zeroed Thick Disk Write Timeout	5400	Eager-zeroed thick disk write timeout for an NFC connection, measured in seconds. This timeout must be larger than the socket timeout of NFC connection. An NFC connection is opened only when interacting with datastore.

VMware Open Virtualization Format Service

The Open Virtualization Format Service enables OVF based provisioning of virtual machines. You can change the configuration properties of this service.

Property	Default Value	Description
OVF Export Session Timeout	5	The amount of time after which the OVF export session times out. Measured in minutes.
OVF Import Session Timeout	10	Waiting time before the OVF import session times out. Measured in minutes.

Image Builder Service

The Image Builder service lets you manage and customize Image Profiles.

Property	Default Value	Description
cachesize_GB	2	Image Builder cache size in gigabytes.
httpPort	8099	Image Builder depot web service port. Cannot be changed.
loglevel	INFO	The default Image Builder log level. Includes information, warnings, errors, and fatal errors.
vmomiPort	8098	Image Builder service API endpoint. Cannot be changed.

VMware Performance Charts Service

The Overview Performance Charts service is a vCenter Server service that collects and processes statistical performance data for managed entities into reports in image format that it provides to the vSphere Web Client.

Property	Default Value	Description
log4j.additivity.com.vmware.vim.common	FALSE	Specifies if the log output from the "com.vmware.vim.common" module should go to its parent appenders.
log4j.additivity.com.vmware.vim.srs	FALSE	Specifies if the log output from the "com.vmware.vim.srs" module should go to its parent appenders.
log4j.additivity.com.vmware.vim.stats	FALSE	Specifies if the log output from the "com.vmware.vim.stats" module should go to its parent appenders.
log4j.appender.CONSOLE1	org.apache.log4j.ConsoleAppender	Defines the "CONSOLE1" appender.
log4j.appender.CONSOLE1.layout	org.apache.log4j.PatternLayout	Specifies the log layout type for the "CONSOLE1" appender.
log4j.appender.CONSOLE1.layout.ConversionPattern	%d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} [%t %x %-5p %c] %m%n	Configures the format of the log messages sent to the "CONSOLE1" appender.
log4j.appender.LOGFILE	com.vmware.log4j.appender.NonAppendingRollingFileAppender	Defines the "LOGFILE" appender.

Property	Default Value	Description
log4j.appender.LOGFILE.Append	true	Specifies if the "LOGFILE" appender output file should be opened in append or truncate mode. True=append, False=truncate.
log4j.appender.LOGFILE.File	${vim.logdir}/stats.log	Configures the path to the file where the "LOGFILE" appender messages should go.
log4j.appender.LOGFILE.layout	org.apache.log4j.PatternLayout	Specifies the log layout type for the "LOGFILE" appender.
log4j.appender.LOGFILE.layout.ConversionPattern	%d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} [%t %x %-5p %c] %m%n	Configures the format of the log messages sent to the "LOGFILE" appender.
log4j.appender.LOGFILE.MaxBackupIndex	10	Sets the maximum number of backup log files to keep.
log4j.appender.LOGFILE.MaxFileSize	5MB	Controls the maximum file size that the log file is allowed to reach before being rolled over to backup files.
log4j.logger.com.vmware.vim.common	INFO, LOGFILE	Configures the logging level and appenders for the "com.vmware.vim.common" module.
log4j.logger.com.vmware.vim.srs	INFO, LOGFILE	Configures the logging level and appenders for the "com.vmware.vim.srs" module.
log4j.logger.com.vmware.vim.stats	INFO, LOGFILE	Configures the logging level and appenders for the "com.vmware.vim.stats" module.
log4j.logger.org.apache	WARN	Configures the logging level and appenders for the "org.apache" module.
log4j.rootLogger	ERROR, LOGFILE	Configures the logging level and appenders for the "log4j.rootLogger" module.

VMware vSphere Authentication Proxy

The VMware vSphere Authentication Proxy service provides support for joining unattended ESXi hosts to an Active Directory domain by using an account with delegated privileges, enhancing security for PXE-booted hosts and hosts that are provisioned using Auto Deploy.

Property	Default Value	Description
Domain	-	Active Directory domain to which to join the ESXi hosts.
Domain User	-	Active Directory account with delegated domain join privileges used to join ESXi hosts.
Domain User Password	-	Password for the account specified in Domain User.

VMware vSphere ESXi Dump Collector

The vSphere ESXi Dump Collector service collects core dumps from remote hosts.

Property	Default Value	Description
Coredump Server UDP Port (1025-9999)	6500	The default port on which the core dump server communicates.
Repository max size (1-10 GB)	2	The maximum size of the core dump repository in gigabytes.

VMware vSphere Update Manager

Provides centralized, automated patch and version management for ESXi hosts and virtual machines.

Property	Default Value	Description
Download patches on service start	true	Controls whether to download patches on service start or not. This option does not take effect when the service starts for the first time after the deployment. This option takes effect on subsequent service starts and restarts.
Log level	INFO	Controls the log messages that vSphere Update Manager will write to its log files.
SOAP Port	8084	The port used by vSphere Update Manager client plug-in to connect to the vSphere Update Manager SOAP server.
Web Server Port	9084	The HTTP port used by ESXi hosts to access host patch files from vSphere Update Manager server.
Web SSL Port	9087	The HTTPS port used by vSphere Update Manager Client plug-in to upload host upgrade files to vSphere Update Manager server.

vAPI Endpoint

The vAPI endpoint provides a single point of access to vAPI services. You can change the properties of the vAPI Endpoint service.

Property	Default Value	Description
[default] endpoint maximum number of execution threads	300	The maximum number of execution threads for the vAPI endpoint.
[default] endpoint minimum number of spare threads	10	The minimum number of threads that are always kept alive for the vAPI endpoint.
[default] endpoint queue size	50	The maximum number of tasks that can queue up for the vAPI endpoint.

Property	Default Value	Description
[router] Broadcast execution timeout	30	The duration after which vAPI broadcast routing queries time out, measured in seconds.
[router] Federated IS queries timeout	30	Timeout of federated inventory service queries, measured in seconds.
[router] Maximum size of the in-memory cache	10	The maximum size of the identifier cache that is used for routing vAPI calls between management nodes. Measured in megabytes.
[router] Number of broadcast timeout threads	3	The number of threads that handle vAPI broadcast time outs.
[router] Number of control threads for federated IS queries	10	The number of threads that control the federated Inventory Service queries for vAPI routing.
[router] Number of execution threads for federated IS queries	20	The number of threads that perform the federated Inventory Service queries for vAPI routing.
Bearer token usage allowance	Enabled	You can use Bearer SAML tokens in addition to Holder of Key (HoK) tokens. Bearer tokens do not have cryptographic verification of the client identity. Their security is sufficient only when used over a secure encrypted connection.
CloudVM Components	authz,com.vmware.cis,com.vmware.content, com.vmware.transfer,com.vmware.vapi,com.vmware.vapi.rest.navigation, com.vmware.vapi.vcenter,com.vmware.vcenter.inventory	A comma-separated list of VMware components that require the use of identifiers. Identifiers must be qualified with a management node ID. The list must not contain spaces. **Caution** Editing the list might result in system failures. Edit this setting only as part of VMware maintenance procedure.
Cookie authentication	Enabled	Enables or disables cookie authentication. If you enable the cookie authentication, the session ID is returned in cookie. If you disable it, the cookie is returned in the header.
Credentials login allowance	Enabled	vAPI users can authenticate with a user name and password in addition to using a SAML token.
Enables REST basic authentication	Enabled	Enables login service for simple authentication with user name and password.
Global request rate	180	Global request rate. Set to 0 to disable.

Property	Default Value	Description
Global request rate interval	1	Global request rate interval, measured in seconds. This is the time frame in which only http.request.rate.count requests are allowed. Set to 0 to disable. If you enable this interval, the default value is 1.
Maximum allowed request size	204800	The maximum allowed request size, measured in bytes. Set to 0 to disable.
Maximum number of in-flight requests.	2000	The maximum allowed number of in-flight requests. Set to 0 to disable. **Note** In-flight requests take up memory. If you increase this setting, you must increase the memory of the endpoint component.
Maximum number of simultaneous connections to the VIM service	10	The max number of simultaneous connections allowed to the VIM service.
Maximum request age	14400	The maximum request age in seconds.
Maximum session count	1000	The maximum number of allowed sessions. If you leave the value empty, the maximum number of sessions allowed is 10,000.
Maximum session idle time	3600000	The maximum time between requests that a session can remain idle, measured in milliseconds.
Maximum session lifespan	172800000	The maximum session lifespan, measured in milliseconds. Used to capture long sessions.
Minimum session lifespan	86400000	Minimum session lifespan in milliseconds, used for renewable tokens.
Reconfiguration interval	240	Interval between reconfiguration attempts, measured in seconds.
Request rate for anonymous calls	3000	Maximum request rate for anonymous calls. Set to 0 to disable.
Request rate for authorized requests	3800	Maximum request rate for authorized calls. Set to 0 to disable.

Property	Default Value	Description
Request rate interval for anonymous calls	60	Request rate interval for anonymous calls, measured in seconds. This is the time frame in which only request rates for anonymous calls are allowed. Set to 0 to disable. **Note** The vAPI endpoint limits the number of incoming requests to Request rate for anonymous calls per Request rate interval for anonymous calls. For example if the rate is set to 50 seconds and interval is set to 60 seconds, the system allows up to 50 calls per minute. Any calls exceeding the limit return a server busy error.
Request rate interval for authorized calls	60	The request rate interval for authorized calls, measured in seconds. This is the time frame in which only http.authorized.request.rate.count authorized requests are allowed. Set to 0 to disable.
The socket timeout	0	The socket timeout (SO_TIMEOUT), measured in milliseconds, that is used when executing a method. A timeout value of 0 is interpreted as an infinite timeout.
Timeout for the HTTP connections to vAPI providers	300000	Timeout for the HTTP connections to vAPI providers, measured in milliseconds.
Token clock tolerance	1000	Clock tolerance for authentication tokens, measured in seconds.
URL Deserialization (POST-as-GET)	Enabled	Enables or disables URL deserialization (POST-as-GET).
vAPI Endpoint solution user	Generated at the time of installation	vAPI Endpoint solution user. **Caution** Do not modify this value. Changing only this setting without updating the related settings, might lead to a failure of the component.

Using Enhanced Linked Mode

4

Enhanced Linked Mode links multiple vCenter Server systems by using one or more Platform Services Controllers. 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 both vCenter Server on Windows and vCenter Server Appliance systems:

- 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 Web 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 Platform Services Controller, or to Platform Services Controllers that share 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.

In vSphere 5.5 and earlier, Linked Mode relied on Microsoft ADAM to provide replication functionality. Starting in vSphere 6.0, the Platform Services Controller provides replication and ADAM is no longer required. Because of the change in architecture, you must isolate vCenter Server 5.5 systems from any Linked Mode groups before upgrading these systems to vCenter Server 6.0. For more information, see the *vSphere Upgrade* documentation.

Configuring Communication Among ESXi, vCenter Server, and the vSphere Web Client

5

By default, the vSphere Web Client uses ports 80 and 443 to communicate with vCenter Server and ESXi hosts.

Configure your firewall to allow communication between the vSphere Web Client and vCenter Server by opening ports 80 and 443.

vCenter Server acts as a web service. If your environment requires the use of a web proxy, vCenter Server can be proxied like any other web service.

Configuring Hosts and vCenter Server

6

Configuring ESXi hosts, vCenter Server systems, and the vSphere Web Client involves several tasks.

This chapter includes the following topics:

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. Select a host in the inventory.
2. Click the **Configure** tab.
3. Select **Processors** and click **Boot Options**.
4. Select a boot device from the drop-down menu.
5. (Optional) To reboot immediately from the device you have 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 is next rebooted.
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 not deployed if you do not configure the network and datastore settings.

Procedure

1. Select a host in the vSphere Client inventory.
2. Click the **Configure** tab.
3. 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 In Advanced System Settings, select the appropriate item.

5 Click the **Edit** button 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 Appliance `vmware-vpxd` service from starting.

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

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

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

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See Knowledge Base article KB 1318.

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

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

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

Edit Time Configuration for a Host

You can configure the time settings on a host manually, or you can synchronize the time and date of the host by using an NTP server.

Procedure

1. In the vSphere Client, navigate to the host in the vSphere inventory.
2. Select **Configure**.
3. Under System, select **Time Configuration** and click **Edit**.
4. Select an option for setting the time and date of the host.

Option	Description
Manually configure the date and time on this host	Set the time and date for the host manually.
Use Network Time Protocol (Enable NTP client)	Synchronize the time and date of the host with an NTP server. The NTP service on the host periodically takes the time and date from the NTP server. a In the **NTP Servers** text box, type the IP addresses or host names of the NTP servers that you want to use. b From the **NTP Service Startup Policy** drop-down menu, select an option for starting and stopping the NTP service on the host. ■ **Start and stop with port usage** - Starts or stops the NTP service when the NTP client port is enabled or disabled for access in the security profile of the host. ■ **Start and stop with host** - Starts and stops the NTP service when the host powers on or shuts down. ■ **Start and stop manually** - Enables manual starting and stopping of the NTP service. You can use the **Start**, **Stop**, or **Restart** buttons to control the status of the NTP service on the host manually at any time. This manual process bypasses the selected startup policy for the NTP service. For the **Start and stop manually** policy, you always use the buttons to control the status of the NTP service.

5. Click **OK**.

Configuring Customer Experience Improvement Program

7

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

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. To join or leave the CEIP for this product, see Join the Customer Experience Improvement Program in the vSphere Web Client.

Join the Customer Experience Improvement Program in the vSphere Web Client

You can choose to join your vCenter Server to the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

Prerequisites

Verify that you are a member of the Administrators@vsphere.local group.

Procedure

1. Log in to the vCenter Server instance as a member of Administrators@vsphere.local group by using the vSphere Web Client.
2. On the vSphere Web Client Home page, under Administration, click **Customer Experience Improvement Program**.

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

What to do next

To leave and rejoin your host to the CEIP, see *Leave and Rejoin the Customer Experience Improvement Program* in the vSphere Single Host Management - VMware Host Client documentation.

Organizing Your Inventory

8

Plan how you will set up your virtual environment. 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. Regardless of the scale of your virtual environment, consider how the virtual machines it will support are going to be used and administered.

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

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

- 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.

Tasks for Organizing Your Inventory

Populating and organizing your inventory involves the following activities:

- Create data centers.
- Add hosts to the data centers.
- Organize inventory objects in folders.

- Set 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, setup VMkernel networking for these services. For more information, see *vSphere Networking*.
- Configure storage systems and create datastore inventory objects to provide logical containers for storage devices in your inventory. See *vSphere Storage*.
- Create 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.
- Create 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 Data Centers

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 sets of environments. For example, you might create a data center for each organizational unit in your enterprise or create some data centers for high-performance environments and others for less demanding virtual machines.

Prerequisites

In the vSphere Client, verify that you have sufficient permissions to create a data center object.

Procedure

1. In the vSphere Client, navigate to the vCenter Server object.
2. Select **Actions > New Datacenter**.
3. Rename 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.

Add a Host

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

You can also add hosts to a DRS cluster, for details see *vSphere Resource Management*.

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 other custom-configured port.
- Verify that all NFS mounts on the host are active.
- 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 x-large environment.

Required privileges:

- **Host.Inventory.Add host to cluster**
- **Resource.Assign virtual machine to resource pool**
- **System.View** on the virtual machines folder where you want to place the virtual machines of the host.

Procedure

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

   To add hosts to a cluster, see *Add Hosts to a Cluster in the vSphere Client*.
2. Right-click the data center, cluster, or folder and select **Add Host**.
3. Type the IP address or the name of the host and click **Next**.
4. Type 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. Type of copy and paste the new license key from My VMware 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.

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**.

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

Create a Folder

You can use folders to group objects of the same type for easier management. For example, permissions can be applied to folders, allowing you to use folders to group objects that should have a common set of permissions.

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

You can create these types of folders: Host and Cluster folders, Network folders, Storage folders, and VM and Template folders.

Procedure

1 In the vSphere Client, select either a data center or another folder as a parent object for the folder.

2 Right-click the parent object and select the menu option to create the folder.

Option	Description
The parent object is a data center.	If the parent object is a data center, you can select the type of folder to create: ■ Select **New Folder > New Host and Cluster Folder**. ■ Select **New Folder > New Network Folder**. ■ Select **New Folder > New Storage Folder**. ■ Select **New Folder > New VM and Template Folder**.
The parent object is a folder.	If the parent object is a folder, the new folder is of the same type as the parent folder. Select **New Folder**.

3 Type the 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 objects by dragging the object to the destination.

Creating 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 within it.

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 create and configure a cluster by either using the vSphere Web Client or through the simplified Quickstart workflow in the vSphere Client. In the **Cluster quickstart** page, there are three cards for configuring your new cluster.

Table 8-1. The cards initiating wizards for renaming and configuring a new cluster.

Cluster Quickstart Workflow	Description
1. `Cluster basics`	Lists the services you have already enabled and allows editing the cluster's name.
2. `Add hosts`	Adds new and already present in the inventory ESXi hosts. Once hosts are added, it shows the total number of the hosts present in the cluster and health check validation for those hosts. In the beginning, this card is empty.
3.`Configure cluster`	Informs you what can be automatically configured, provides details on configuration mismatch, and reports cluster health results through the vSAN Health service even after the cluster is configured.

The **Skip Quickstart** button prompts you to continue configuring the cluster and its hosts manually. You click **Continue** to confirm exiting the simplified configuration workflow. Once dismissed, there is no option to restore the **Cluster quickstart** workflow for the current cluster.

Clusters enable vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), and the VMware vSAN features.

Create Clusters in the vSphere Client

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

Follow the steps to create and configure a new cluster with default settings. To use the vSAN service, turn on vSAN and see *Administering VMware vSAN* documentation.

Prerequisites

- Verify that you have sufficient permissions to create a cluster object.
- Verify that a data center, or 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 or networking configuration.

Procedure

1. Navigate to **Home > Hosts and Clusters** and select a data center.
2. Right-click the data center and select **New Cluster**.
3. Enter a name for the cluster.
4. Select DRS and vSphere HA 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. You are present with the following default values: Automation Level: Fully Automated Migration Threshold: 3
To use 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: Host Monitoring: Enabled Admission Control: Enabled VM Monitoring: Disabled

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

5. Click **OK**.

   The cluster appears in the vCenter Server inventory. You are present with the **Quickstart** service under the **Configure** tab.

6. (Optional) Click **Edit** in the **Cluster basics** card to rename your cluster and to enable or disable cluster services.

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

What to do next

Add hosts to the cluster.

Add Hosts to a Cluster in the vSphere Client

You add hosts to your cluster by launching the **Add hosts** wizard, part of the Cluster quickstart workflow.

Follow the steps to add new and existing ESXi hosts in the vCenter Server inventory.

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 or networking configuration.

Procedure

1. Click **Add** in the **Add hosts** card.
2. On the **Add hosts** page, under the **New hosts** tab, add hosts that are not part of the vCenter Server inventory by populating the IP Address and credentials text boxes for those hosts.
3. (Optional) Select the `Use the same credentials for all hosts` option to reuse the credentials for all added hosts.

   You enable this option after populating the first line of credentials.
4. On the **Add hosts** page, click the **Existing hosts** tab, and add hosts that are managed by the vCenter Server and are in the same data center as your 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. Click **Next**.
7. On the **Ready to complete** page, review the added hosts and click **Finish**.

   The number of added hosts and the health check validation, performed by the vSAN Health service, are summarized in the **Add hosts** card.
8. (Optional) Click **Re-validate** to retrigger the validation of the hosts.

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

All hosts are placed in maintenance mode and added to your cluster.

What to do next

Configure your cluster default settings through the Quickstart workflow.

Configure a Cluster in the vSphere Client

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

Follow the steps to configure the default settings of your cluster.

Note To configure your cluster host networking and services manually by referring to different parts of the vSphere software, click the **Skip quickstart** button. By dismissing the **Cluster quickstart** workflow, you cannot restore it and hosts added to this cluster in the future have to be configured manually.

Prerequisites

Procedure

1 In the **Configure cluster** card, select **Configure**.

2 In the **Distributed switches** page, complete the host networking.

Alternatively 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. You cannot perform the networking configuration in 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 will connect to them.

b Name differently 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**.

If you enabled the vSphere DRS feature during cluster creation, the **vMotion traffic** page appears.

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

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

i (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.

3 Click **Next**.

The **Advanced options** page appears.

4 (Optional) If you enabled the vSphere HA feature during cluster creation, the **High Availability** section is visible.

   a Enable or disable host failure monitoring.

   b Enable or disable virtual machine monitoring.

   c Enable or disable admission control.

      If enabled, specify the failover capacity by number of hosts.

5 (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.

6 In the **Host Options** section, set the Lockdown mode to `Strict`, `Normal` or `Disabled`, and enter an NTP server address.

   The settings are applied across all hosts in this cluster.

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

8 Click **Next**.

   The **Ready to complete** page appears.

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

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

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

What to do next

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

Extending Clusters

You extend a configured cluster by adding hosts to it. With vSphere 6.7, you use the **Cluster quickstart** workflow in the vSphere Client.

After you have configured your cluster, you can scale it out by adding more hosts. Then, you specify the network configuration for the new hosts in the cluster. If during the initial configuration of the cluster you have 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 same configuration of the existing hosts in the cluster is applied to the new hosts.

Prerequisites

- You have already created a cluster and added hosts to it.
- In the initial cluster configuration, you selected the `Configure networking settings later` check box.
- 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.

Procedure

1. Navigate to **Home > Hosts and Clusters** and select a configured cluster.
2. Right-click the cluster and select **Add Hosts**.
3. From the **Add hosts** wizard, add new and existing hosts from the vCenter Server inventory.

   The **Cluster quickstart** page appears.
4. In the Configure cluster card, click **Configure**.

   A pop-up window appears. It informs you that the configuration for the existing in the cluster hosts is applied on the newly added hosts.
5. Select **Continue**.

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 manually the host networking 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

- You have already created a cluster and added hosts 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 or networking configuration.

Procedure

1. Navigate to **Home > Hosts and Clusters** and select a configured cluster.
2. Right-click the cluster and select **Add Hosts**.

3 From the **Add hosts** wizard, add new and existing hosts from the vCenter Server inventory.

   The **Cluster quickstart** page appears.

4 In the **Configure cluster** card, select **Configure**.

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

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

   b (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 **Ready to complete** page appears.

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

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

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

9

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:

Migrate Custom Attributes to Tags

Tags replace the custom attributes functionality found in previous versions of vSphere. If you have existing custom attributes, you can migrate them to tags.

During the migration, the custom attribute names are converted to categories. Custom attribute values are converted to tag names.

Procedure

1. In the vSphere Web Client object navigator, browse to any object that has custom attributes.
2. Click the object's **Summary** tab.
3. Select **Actions > Tags & Custom Attributes > Edit Custom Attributes...**
4. In the Migrate Custom Attributes dialog box, click **Migrate**.

   The **Migrate Custom Attributes to Tags** wizard appears.
5. Read the instructions and click **Next**.
6. Select the custom attributes to migrate and click **Next**.

   The Create Tag Categories page displays the name of each custom attribute as a new tag category.
7. (Optional) Select a category to edit its 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.
Cardinality	■ Select **One tag per object** to allow only one tag from this category to be applied to an object at any one time. Use this option for categories whose tags are mutually exclusive. For example, a category called Priority with tags High, Medium, and Low should allow one tag per object, because an object should have only one priority. ■ Select **Many tags per object** to allow multiple tags from the category to be applied to an object at any one time. Use this option for categories whose tags are not mutually exclusive. After you have set the cardinality of a category, you can change the cardinality from **One tag per object** to **Many tags per object**, but not from **Many tags per object** to **One tag per object**.
Associable Object Types	Select whether tags in this category can be assigned to all objects or only to a specific type of managed object, such as virtual machines or datastores. After you have set the associable object types for a category, you can change a category that is associable with a single object type to be associable with all object types. You cannot restrict a category that is associable to all object types to being associable to a single object type.

8 (Optional) Select a tag to edit its attributes.

Option	Description
Name	The tag name must be unique across all linked vCenter Server systems.
Description	You can provide text in the description to describe the purpose or use of the tag.

9 Click **Finish**.

The selected custom attributes are converted to categories and tags.

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.

Prerequisites

The required privilege depends on the task that you want to perform.

Task	Privilege
Create a tag category	**vSphere Tagging.Create vSphere Tag Category** on the root vCenter Server
Edit a tag category	**vSphere Tagging.Edit vSphere Tag Category** on the root vCenter Server.
Delete a tag category	**vSphere Tagging.Delete vSphere Tag Category** on the root vCenter Server.

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, Edit, or Delete a Tag

You 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.

Prerequisites

The required privilege depends on the task that you want to perform.

Task	Privilege
Create a tag	**vSphere Tagging.Create vSphere Tag** on the root vCenter Server
Edit a tag	**vSphere Tagging.Edit vSphere Tag** on the root vCenter Server
Delete a tag	**vSphere Tagging.Delete vSphere Tag** on the root vCenter Server

Procedure

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

2 Click **Tags**.

3 Perform the task.

Option	Description
Create a tag	a Click the New Tag icon. b Specify the **Name** and an optional **Description**. c In the **Category** drop-down menu, select an existing category or create a category. If you select **[New Category]**, the dialog box expands to show the options for creating a category. See Create, Edit, or Delete a Tag Category.
Edit a tag	Select a category and click the **Edit Category** icon.
Delete a tag	Select a category from the list and click the **Delete Category** icon.

4 Click **OK**.

Assign or Remove a Tag

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

Prerequisites

Required privilege: **vSphere Tagging.Assign or Unassign vSphere Tag** on the root vCenter Server instance

Procedure

1 Browse to the object in the vSphere Client inventory.

2 From the Actions menu, select **Tags and Custom Attributes > Assign Tag**.

3 Select a tag from the list and click **Assign**.

You can later use the same process to remove a tag.

4 From the Actions menu, select **Tags & Custom Attributes > Remove Tag**.

5 Select a tag from the list and click **Remove**.

Add Permissions for Tags and Tag Categories

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

You can set permissions on common tag operations to manage the operations over the inventory objects. You must have vSphere administrator credentials to set and manage permissions for tags. 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.

Permissions for tags work similar to permissions for vCenter Server inventory objects. See *vSphere Security* for more background information.

Procedure

1. In the vSphere Web Client, select **Menu > Tags & Custom Attributes**.
2. Select a tag from the list, right-click the tag, and select **Add Permission**.

   You see a list with all default permissions for the selected tag.
3. Click the Add icon to add a permission to the existing list.

   The Add permission dialog box appears.
4. In the Users and Groups pane, click **Add**, select all the users and groups you want to add, and click **OK**.
5. (Optional) Select a user or a group from the list and select a role from the **Assigned Role** list.
6. (Optional) Select **Propagate to children** to propagate the privileges to the children of the assigned inventory object.
7. Click **OK** to save the new tag permission.

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 in the vSphere Web Client

You can use custom attributes in the vSphere Web 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.

Prerequisites

Required privileges: **Global.Manage custom attributes**,**Global.Set custom attribute**.

Procedure

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

2 Click **Custom Attributes**.

All currently defined custom attributes for vCenter Server are displayed.

3 Click **Add**.

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**.

License Management and Reporting

10

vSphere provides a centralized license management and reporting system that you can use to manage licenses for ESXi hosts, vCenter Server systems, vSAN 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 6.7

  In vSphere 6.7, the License Service is part of the Platform Services Controller. 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, and vSAN clusters are licensed differently. To apply their licensing models correctly, you must understand how the associated assets consume 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, vSphere with Operations Management, and VMware vSphere Platinum.

- 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 and the vSphere Web Client to license multiple assets at a time from a central place. Assets are vCenter Server systems, hosts, vSAN 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 or the vSphere Web 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.

- Generating Reports for License Use in the vSphere Web Client

  You can track the license use of your vSphere environment by generating reports for the license use of assets for a certain time period. Assets are hosts, vCenter Server systems, vSAN clusters, and solutions.

- Synchronizing Licenses with Your My VMware Account

  With vSphere 6.5 and later, VMware starts offering the Synchronize Licenses feature that you can use to import license keys and license key data from My VMware 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 Web Client or 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, VMware vSphere Platinum, 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 6.7

In vSphere 6.7, the License Service is part of the Platform Services Controller. 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, and clusters with enabled vSAN. 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 Platform Services Controllers that are joined through one vCenter Single Sign-on domain, the licensing inventory is replicated across all Platform Services Controllers. This way, the licensing data for each asset and all available licenses are replicated across all the Platform Services Controllers. Each individual Platform Services Controller contains a copy of that data and licenses for all the Platform Services Controllers.

Note Licensing data is replicated across multiple Platform Services Controllers on a 10-minute interval.

For example, suppose that your environment consists of two Platform Services Controllers that are connected to four vCenter Server systems each, 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. The License Service also lets you manage the licensing for all eight vCenter Server systems and the 80 hosts that are connected to them through the vSphere Web 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 interfaces in the vSphere Client 6.7 and the vSphere Web Client 6.0 and later allow 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, and vSAN clusters are licensed differently. To apply their licensing models correctly, you must understand how the associated assets consume 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 CPU capacity that you can use to license multiple physical CPUs on ESXi hosts. When you assign a vSphere license to a host, the amount of CPU capacity consumed equals the number of physical CPUs in the host. 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 CPU capacity to license all physical CPUs on the host. For example, to license two ESXi hosts that have four CPUs each, you need a vSphere license with a minimum capacity of 8 CPUs to the hosts.

- 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.

You can assign and reassign the CPU capacity of a vSphere license to any combination of ESXi hosts. You can assign a vSphere license for 10 CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts
- Three 2-CPU hosts and one 4-CPU host
- Two 4-CPU hosts and one 2-CPU host
- One 8-CPU host and one 2-CPU host

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

When you install ESXi, its default license is evaluation mode. Evaluation mode licenses expire 60 consecutive days after the product is installed. An evaluation mode license provides the set of features that equals the highest vSphere product edition.

If you assign a license to an ESXi host before its evaluation period expires, the time available in the evaluation period decreases by the time already used. To explore the entire set of features available for the host, set it back to evaluation mode, and use it 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 then set the host back to evaluation mode, you can explore the entire set of features available for the host for the remaining evaluation period of 40 days.

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 while the host was in evaluation mode.

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 need to license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license usage 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.

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 Enabled vSAN

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.

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, vSphere with Operations Management, and VMware vSphere Platinum.

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.

Licensing for the VMware vSphere® Platinum Edition

VMware vSphere® Platinum is an edition that combines under a single license the capabilities of vSphere and VMware AppDefense.

VMware vSphere Platinum includes the following components:

- VMware vSphere for Platinum Edition
- VMware AppDefense Plugin for Platinum Edition
- VMware AppDefense (SaaS) for Platinum Edition

VMware AppDefense enhances the security of your environment and protects your applications by monitoring for changes in their intended state. The VMware AppDefense plug-in is a plug-in that you can install, upgrade, and manage only if you have the VMware vSphere Platinum license. When you add a license key for VMware vSphere Platinum, the AppDefense icon appears in the left navigation pane of the vSphere Client. For more information about VMware AppDefense, see the *VMware AppDefense* documentation.

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 and the vSphere Web Client to license multiple assets at a time from a central place. Assets are vCenter Server systems, hosts, vSAN 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 My VMware, you must use the new keys to license assets in your vSphere environment. You must go to the vSphere Client or the vSphere Web Client and create a new 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 or the vSphere Web 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**.

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 Web 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 My VMware, 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, Virtual SAN 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 My VMware, 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, 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 or the vSphere Web 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**, **Clusters**, or **Solutions** tab.
5. Select the assets to license.

   Note In the vSphere Client, 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**.

- In the vSphere Web 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 **Create New License** () icon. b In the **New Licenses** dialog box, type or copy and paste a license key and click **Next**. c On the **Edit license names** page, enter a name for the new license and click **Next**. d Click **Finish**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

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 My VMware, 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 or the vSphere Web 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**.

- In the vSphere Web 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 **Create New License** () icon. b In the **New Licenses** dialog box, type or copy and paste a license key and click **Next**. c On the **Edit license names** page, enter a name for the new license and click **Next**. d Click **Finish**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

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 My VMware, 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 or the vSphere Web Client runs.

Procedure

1 Navigate to the vCenter Server system.

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**.

- In the vSphere Web 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 **Create New License** () icon. b In the **New Licenses** dialog box, type or copy and paste a license key and click **Next**. c On the **Edit license names** page, enter a name for the new license and click **Next**. d Click **Finish**. e In the **Assign License** dialog box, select the newly created license, and click **OK**.

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 that 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.

Option	Description
vSphere Client	a Right-click your vSAN cluster, and choose menu Assign License. b Select a licensing option. ■ Select an existing license and click **OK**.
vSphere Web Client	a Under **Configuration**, select **Licensing**, and click **Assign License**. b Select a licensing option. ■ Select an existing license 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 or the vSphere Web 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**, **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.

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 or the vSphere Web 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 My VMware, you must remove the old licenses.

For example, suppose that you have upgraded a vSphere license from 6.5 to 6.7 in My VMware. You assign the license to ESXi 6.7 hosts. After assigning the new vSphere 6.7 licenses, you must remove the old vSphere 6.5 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 or the vSphere Web 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.

Client	Options
vSphere Client	■ Click the filter icon (▿) in the **State** column. A text box appears. ■ Select what licenses you want to display (unassigned or assigned).
vSphere Web Client	From the **Show** drop-down menu, select **Unassigned** to display only the unassigned licenses.

5 Select a license to remove or press Ctrl+A to select all licenses.

6 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 or the vSphere Web 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 or the vSphere Web 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 or the vSphere Web 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, and other products that you use with vSphere that are listed under Solutions.

What to do next

To comply with the EULA of vSphere and the products that you use with vSphere, you should not keep unassigned licenses in the inventory.

- If any unassigned licenses exist, assign these licenses to assets.
- Remove all expired licenses or licenses that you do not intend to assign. For example, if you have upgraded, divided, or combined any licenses in My VMware, you must remove the old licenses 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 Web 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 or the vSphere Web 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. ■ In the vSphere Web Client, click the arrow next to the product name to expand the row and see a list of all licenses for the respective product.
View the licensed features for the product	■ In the vSphere Client, click the **Features** subtab below the list of products. ■ In the vSphere Web Client, click the **View Features** toolbar icon.

View the Features That an Asset Uses

You can view the features that an asset uses before you assign it a license. For example, if an ESXi host is in evaluation mode, you can view which features the hosts uses and then assign an appropriate license 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 or the vSphere Web 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**, **Clusters**, or the **Solutions** option.
5. Select an asset and view the associated features.
   - In the vSphere Client, click the **Features** subtab below the list of assets.
   - In the vSphere Web Client, click the **View Licensed Features** toolbar icon.

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 or the vSphere Web 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.
   - In the vSphere Client, 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.
   - In the vSphere Web Client, click the **View License Key** toolbar icon.

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 or the vSphere Web 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**.

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 export licensing information in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client or the vSphere Web 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.
vSphere Web Client	a At the bottom right of the list, click the **Export** ( ) icon. b To export the selected item or items, click **Export > Selected Items Only**. c To export all items of the respective type, click **Export > All Items**. d In the **Save As** dialog box, select a folder, a filename, and a format for the exported license data and click **Save**.

Generating Reports for License Use in the vSphere Web Client

You can track the license use of your vSphere environment by generating reports for the license use of assets for a certain time period. Assets are hosts, vCenter Server systems, vSAN clusters, and solutions.

You can use the license reporting in vSphere for the following tasks:

- View statistics about the license use and capacity for all products that have been assigned licenses in vSphere for a certain time period.
- Export license use reports in CSV format for further analysis and processing.

The License Service takes snapshots of the license use in the vSphere environment every day. A license use snapshot contains data about the current license assignment and use. The license use information that you can view in the license reporting interface contains aggregated statistics from the snapshots that are collected in the period that you select.

The license use reports that you can export in CSV format contain the raw data from the license use snapshots that are collected during the selected period. You can analyze the data from CSV reports by aggregating it with third-party tools or scripts.

View the License Usage for Multiple Products in the vSphere Web Client

Tracking the license usage for products helps you to estimate the overall license requirements for your environment and to keep it correctly licensed. You can filter the license usage data by time period.

Prerequisites

- To view and generate license use reports for the products in vSphere, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Web Client runs.

Procedure

1. In the vSphere Web Client navigator, select **Administration**, and under **Licensing** select **Reports**.
2. On the **Products** tab, use the **Time period** drop-down menu to select a preconfigured or a custom time period for which you want to generate license use data.
3. If you select a custom time period, select the start and end dates, and click **Go**.

The Report Summary shows the license usage for each product as a percentage of the license capacity for the product over the selected period.

View License Usage Details for a Single Product in the vSphere Web Client

You can view details about the license usage and capacity of a certain product. You can filter the license usage data by time period.

Prerequisites

- To view and generate license use reports for the products in vSphere, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Web Client runs.

Procedure

1. In the vSphere Web Client navigator, select **Administration**, and under **Licensing** select **Reports**.
2. On the **Products** tab, use the **Time period** drop-down menu to select a preconfigured or a custom time period for which you want to generate license use data.
3. If you select a custom time period, specify the start and end dates, and click **Go**.
4. Select a product from the **Report Summary** pane.

Details about the license usage for the selected product appear. The Usage Breakdown table lists all the licenses for the product that are assigned to assets in the selected period. The table can list licenses that are not used currently but were assigned to assets in the selected period.

The License Service collects license usage snapshots every day. The license usage on the Usage Breakdown table is an aggregated value from the raw data in the license usage snapshots that are collected within the selected time period.

Export a License Usage Report in the vSphere Web Client

You can export a report for the license usage of products for a certain time period. The report is exported in a CSV file that you can later open with third-party applications.

Important A tamper-detection feature in the License Service protects the license usage information. If the licensing data in the License Service database has been edited, you cannot export a license usage report.

Prerequisites

- To export license usage reports, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Web Client runs.

Procedure

1. In the vSphere Web Client navigator, select **Administration**, and under **Licensing** select **Reports**.
2. On the **Products** tab, Click **Export License Usage Report**.

   The **Export License Usage Report** dialog box appears.
3. Select a preconfigured or a custom time period for the license usage report from the **Time period** drop-down menu.
4. Click **Generate CSV report**.

   The operation takes a few seconds.
5. Click **Save** and specify a location where to save the file.

The license usage for products over the selected time period is exported in a CSV file. The CSV file is contained in a `.zip` file that is saved to the location that you specified.

The exported report contains raw data about the license usage of products over the selected period. The rows of the exported CSV file list the license usage snapshots that the License Service has collected daily over the selected period. You can use third-party tools to open the CSV report and analyze its data.

A license usage snapshot contains data about the assigned licenses, associated products, license expiration date, license units (cost units), capacity, usage, asset ID, and so on. Permanent licenses do not have an expiration date listed. vCloud Suite is licensed on per CPU basis, and so, the license usage for vCloud Suite products is reflected only for ESXi hosts that are assigned licenses from the corresponding vCloud Suite editions.

Synchronizing Licenses with Your My VMware Account

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

The Synchronize Licenses feature helps you keep your vCenter Server license keys data synchronized with the license keys data in My VMware. To import license keys data, you use a `.CSV` file that you generate in the My VMware reports section. After you import the `.CSV` file, you can view the My VMware data in the License List and the License Summary.

With the import feature, you can complete the following tasks:

- Add or update My VMware license keys details, such as notes, custom labels, contracts, orders, and so on, in your vCenter license inventory.
- Add license keys from My VMware to your vCenter license inventory.
- Identify any license keys in your vCenter license inventory that have been combined, divided, upgraded, or downgraded in My VMware 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 My VMware account to your vSphere environment.

Prerequisites

Generate a Products, Licenses, Details, and History report in your My VMware account and upload it to vSphere. See Generate a CSV File in My VMware.

Procedure

1 Generate a CSV File in My VMware

To update your vCenter license inventory with the license keys details in your My VMware environment, generate a Products, Licenses, Details, and History `.CSV` file in your My VMware reports section. Upload the `.CSV` file to vSphere.

2 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 My VMware environment, review the results from the `.CSV` file analysis.

Procedure

1 Click **Menu > Administration**.

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

3 Follow the prompts in the **Synchronize Licenses** wizard or the **Import License Keys Data** wizard.

Client	Steps
vSphere Client	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 My VMware environment. **Important** 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 My VMware. 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, seeUsing 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 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 My VMware, download the `Combined_Split_Upgraded_and_Downgraded_License_Keys.csv` report. For information how to manually remove 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 My VMware, download the `Upgraded_License_Keys.csv` report. For information how to manually upgrade your assets, change your license assignments, and remove the upgraded license keys, seeUpgrade License Keys in Your vCenter License Inventory.

Client	Steps
	g On the Ready to complete page, review the import process summary and click **Finish**.
vSphere Web Client	a On the **Licenses** tab, click the **Import License Keys Data** toolbar icon. The **Import License Keys Data** wizard opens. b On the About this feature page, learn about the tasks that you can complete with the wizard and click **Next**. c On the Upload Import File page of the **Import License Keys Data** wizard, click **Browse** 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 My VMware environment. **Important** 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 My VMware. 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, seeUsing CSV Files . d 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. e (Optional) On the Add license keys page, select license keys to add to 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. f (Optional) To remove license keys in your vCenter license inventory that have been combined, split, upgraded, or downgraded in My VMware, download the `Combined_Split_Upgraded_and_Downgraded_License_Keys.csv` report. For information how to manually remove license keys that have been combined, split, upgraded, or downgraded, see Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded. g (Optional) To upgrade license keys in your vCenter license inventory that have upgrade keys available in My VMware, download the

Client	Steps
	`Upgraded_License_Keys.csv` report. For information how to manually upgrade your assets, change your license assignments, and remove the upgraded license keys, seeUpgrade License Keys in Your vCenter License Inventory. h On the Ready to complete page, review the import process summary and click **Finish**.

Generate a CSV File in My VMware

To update your vCenter license inventory with the license keys details in your My VMware environment, generate a Products, Licenses, Details, and History `.CSV` file in your My VMware reports section. Upload the `.CSV` file to vSphere.

The `.CSV` file is a list of keys that are active keys in My VMware. The `.CSV` file contains up-to-date license keys information from your My VMware 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 MyVMware home page, click **Reports** in the top right corner.
3. In the **Select a Report** section, click **Available Reports** and select **Products, Licenses, Details, and History**.
4. In the **Select Accounts** section, select the account, for which you want to generate the report.
5. (Optional) Enter a name for your report.
6. (Optional) Add notes to include in your report.
7. (Optional) To receive an email when the report is ready, select **Send email when report is created**.
8. 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.
9. To download the `.CSV` file that you must import to vSphere, 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 My VMware environment, review the results from the `.CSV` file analysis.

After you upload the .CSV file that you generated in My VMware 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 My VMware.
- 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 My VMware 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 My VMware:

- Update license keys in your vCenter license inventory with details from your My VMware, 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 My VMware, 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 My VMware, 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 My VMware, 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 My VMware. 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 My VMware. To view what keys in your vCenter license inventory have upgrade keys available in My VMware, 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 **Import License Keys Data** 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 My VMware 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 My VMware 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 manually update your vSphere license inventory.

Note The recommendation reports are only available on the Ready to complete page of the **Import License Keys Data** wizard. Download the reports to manually perform the actions.

For information how to remove from your vSphere license inventory existing license keys that have been combined, divided, upgraded, or downgraded in My VMware, see Remove License Keys That Have Been Combined, Divided, Upgraded, or Downgraded.

For information how to manually upgrade your assets, change your license assignments, and remove license keys from your vCenter license inventory that have upgrade keys available in My VMware, 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 My VMware, use the generated recommendation

Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv report to manually remove these license keys.

When you add license keys to your vCenter license inventory that the system proposes on the Add license keys page of the **Import License Keys Data** 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 My VMware, 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 **Import License Keys Data** wizard.

Procedure

1. In the vSphere Web Client navigator, select **Administration**, and under **Licensing**, select **Licenses**.
2. Select the **Licenses** tab.
3. Open your Combined_Divided_Upgraded_and_Downgraded_License_Keys.csv file and locate the **Inactive Key in Use in vCenter** column.
4. View the inactive key in the .CSV file, select that same key in the **Licenses** tab in the vSphere Web 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 My VMware.

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 My VMware, use the generated recommendation .CSV file report to manually upgrade your assets, 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 **Import License Keys Data** 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 My VMware, 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 **Import License Keys Data** wizard.

Procedure

1. In the vSphere Web Client navigator, select **Administration**, and under **Licensing**, select **Licenses**.
2. Select the **Licenses** tab.
3. Open your `Upgraded_License_Keys.csv` file and locate the **Inactive Key in Use in vCenter** column.
4. View the inactive key in the `.CSV` file, select that same key in the **Licenses** tab in the vSphere Web 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 External Platform Services Controller 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.

Working with Tasks

11

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

This chapter includes the following topics:

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 11-1. 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 Update 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 Update 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 Web 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 Web Client, navigate to the object for which you want to schedule a task.
2. Select **Monitor**, and select **Tasks & Events**.
3. Select **Scheduled Tasks** from the list on the left.
4. From the **Schedule New 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.

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

a Type a name and a description for the task.

b To configure the scheduling settings for the task, click **Change** next to Configured Scheduler.

Table 11-2. Scheduler options

Option	Description
Run this action now	Runs the scheduled task immediately.
Run this action after startup	Runs the task after a certain number of minutes.
Schedule this action to run later	Runs the scheduled task at a date and time that you specify.
Setup a recurring schedule for this action	Runs the scheduled task on a recurring pattern.
Hourly	1 Type the number of hours after which to run the task. 2 Type the number of minutes after the hour to run the task. 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 number of days on which to run the task. 2 Type the start time for the task. For example, to run the task at 2:30 pm every four days, type **4** and **2:30**.
Weekly	1 Type the number of weeks on which the task must run. 2 Select the day of the week you want the task to run. 3 Type the start time for the task. 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 start time for the task. 2 Select the days by using one of the following methods. ■ Type a specific day of the month and the number of months to run the task. 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 to run the task. **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**.

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 Web 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 **Monitor**, and select **Tasks & Events**.
3. Select **Scheduled Tasks** from the list on the left.
4. Right-click the task and select **Edit**.
5. Change the task attributes as necessary.
6. Click **OK**.

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 Web 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 **Monitor**, and select **Tasks & Events**.
3. Select **Scheduled Tasks** from the list on the left.
4. Right-click the task to remove and select **Remove**.

Managing Hosts in vCenter Server

12

To access the full capabilities of the host that you are managing, connect the host 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

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 in the vSphere Web Client 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 Server cannot 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 will be encrypted and stored in the database using the new certificate.

Relocate a Host

When a host is removed from a cluster, the resources it provides are deducted from the total cluster resources. The virtual machines deployed on the host are either migrated to other hosts within the cluster, or remain with the host and are removed from the cluster, depending on the state of the virtual machines when the host is removed from the cluster.

You can remove hosts from a cluster by selecting them in the inventory and dragging them to a new location within the inventory. The new location can be a folder as a standalone host or another cluster.

Prerequisites

Before you can remove a host from a cluster, you must power off all virtual machines that are running on the host, or migrate the virtual machines to a new host using vMotion.

Procedure

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

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

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

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

     If the host is inside a DRS-enabled cluster, entering maintenance mode causes DRS to attempt to evacuate powered-on virtual machines from the host using vMotion.

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

     The confirmation dialog box also asks if you want to evacuate virtual machines that are not powered on from the host. This is useful if you want those virtual machines to remain registered to a host within the cluster.

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

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

   The host can be moved to another cluster or another data center.

   vCenter Server moves the host to the new location.

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

5 (Optional) Restart any virtual machines, as needed.

Remove a Host from vCenter Server

Remove a managed host from vCenter Server to stop all vCenter Server monitoring and management of 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.

Procedure

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

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

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

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

     If the host is inside a DRS-enabled cluster, entering maintenance mode causes DRS to attempt to evacuate powered-on virtual machines from the host using vMotion.

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

     The confirmation dialog box also asks if you want to evacuate virtual machines that are not powered on from the host. This is useful if you want those virtual machines to remain registered to a host within the cluster.

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

3 If the host is connected to a distributed switch, first you must remove the host from the switch.

   For more information, see "Remove Hosts from a vSphere Distributed Switch" in the *vSphere Networking* documentation.

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

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

   vCenter Server removes the host and associated virtual machines from the vCenter Server environment. 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 host disconnects it from vCenter Server, but does not remove it from the inventory.

Procedure

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

2 Power off all virtual machines running on the ESXi host.

3 Right-click the ESXi host and select **Power** > **Reboot** or **Power** > **Shut Down**.

   - If you select **Reboot**, the ESXi host shuts down and reboots.
   - If you select **Shut Down**, the ESXi host shuts down. You must manually power the system back on.

4 Provide a reason for the reboot or shut down operation and click **Ok**.

   This information is added to the log.

Migrating Virtual Machines

13

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 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. For information about the requirements about vMotion across vCenter Server instances, see Requirements for Migration Between vCenter Server Instances.

This chapter includes the following topics:

- Migrate a Powered-Off or Suspended Virtual Machine in the vSphere Web Client
- Migrate a Virtual Machine to a New Compute Resource
- Migrate a Virtual Machine to a New Compute Resource and Storage in the vSphere Web Client
- Migrate a Virtual Machine to New Storage in the vSphere Web Client
- 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 6.0 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 allows 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 the VMware KB article at http://kb.vmware.com/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 VMware knowledge base article at http://kb.vmware.com/kb/1003832. For information about configuring advanced settings of vCenter Server, see Configure Advanced Settings .

For information about configuring the vMotion network resources, see Networking Best Practices for vSphere vMotion .

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.

- 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 the configuring networking on an ESXi host, see the *vSphere Networking* documentation.

Encrypted vSphere vMotion

Starting with vSphere 6.5, 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 virtual machines across vCenter Server instances.
- vSphere does not support vMotion of encrypted virtual machines across vCenter Server instances. Because one vCenter instance cannot verify that another vCenter instance is connected to the same Key Management System cluster, the proper encryption keys are not available for successful VM encryption operation. As a result, vMotion in this situation is not currently supported.

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**.

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.
- 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.
- You can migrate virtual machines that use Flash Read Cache if the destination host also provides Flash Read Cache. During the migration, you can select whether to migrate the virtual machine cache or drop it, for example, when the cache size is large.

Using vMotion to Migrate vGPU Virtual Machines

You can use vMotion to perform a live migration of NVIDIA vGPU-powered virtual machines without causing downtime or data loss.

In vSphere 6.7 Update 1 and later, vGPU vMotion is supported for vGPU profiles of up to 12 GB of frame buffer. The 12GB frame buffer limit represents a single vGPU device attached to the VM, regardless of the GPU model or vGPU profile. Attempts to migrate VMs with vGPU frame buffers exceeding this limit might exceed the 100 second timeout for vSphere vMotion stun time, resulting in the migration process failing due to timeout.

While the migration is in progress, you will be unable to access the VM, desktop, or application. Once the migration is completed, access to the VM will resume and all applications will continue from their previous state. If the migration fails, the VM remains on the source host. To preserve the application (and GPU) state during the cold-migration of VMs with a vGPU frame buffer over 12 GB, the VM should be suspended, cold migrated, and resumed on a compatible destination host. 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 P40 GPUs :

Table 13-1. Expected Stun Times for vMotion of vGPU VMs

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
1	9.0
2	16.5
4	31.4
8	61.3
10	76.3
12	91.2

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
16	100+ (vMotion timeout)
24	100+ (vMotion timeout)

Note The configured vGPU profile represents an upper bound to the used vGPU frame buffer. In many VDI/Graphics 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, an M60-8A vGPU profile will allocate 8 GB of vGPU frame buffer to the VM, but the VM can use any amount between 0-8GB of frame buffer during the migration. This means that the stun time can end up being between less than 1 sec to 61.3 seconds.

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 6.0 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 6.0 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 source cluster's storage. 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 off a host to allow maintenance of the host.
- Storage maintenance and reconfiguration. You can move virtual machines off 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.

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 source and destination vCenter Server instances and ESXi hosts must be 6.0 or later.
- 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.
- 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.
- When using the vSphere Web Client, both vCenter Server instances must be in Enhanced Linked Mode and must be in the same vCenter Single Sign-On domain. This lets the source vCenter Server to authenticate to the destination vCenter Server.

  For information about installing vCenter Server in Enhanced Linked Mode, see the *vCenter Server Installation and Setup* documentation.

  If the vCenter Server instances exist in separate vCenter Single Sign-On domains, you can use vSphere APIs/SDK to migrate virtual machines. For more information, see the VirtualMachineRelocateSpec data object in the *VMware vSphere API Reference*.

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 black list so that it does not assign them to newly created virtual machines.

To reclaim unused MAC addresses from the black list, contact VMware Technical Support for assistance.

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 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
- ESX/ESXi version running on the host
- The virtual machine's compatibility setting
- The virtual machine's guest operating system

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.

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 two hosts' user-level features blocks migration, whether or not the virtual machine itself has access to those features. A mismatch between two hosts' kernel-level features 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 virtual machine's CPU feature set. CPU compatibility requirements are met, and migration with vMotion proceeds.
- The virtual machine's CPU feature set 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 virtual machine's feature set, plus additional user-level features (such as SSE4.1) not found in the virtual machine's feature set. 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 virtual machine's feature set, plus additional kernel-level features (such as NX or XD) not found in the virtual machine's feature set. 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*.

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 6.0 or later.
vCenter Server	The host must be connected to a vCenter Server system.
CPUs	A single vendor, either AMD or Intel.

Requirements	Description
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.

Create an EVC Cluster

Create an EVC cluster to ensure vMotion CPU compatibility between the hosts in the cluster.

To create an EVC cluster with minimal disruption to your existing infrastructure, create an empty EVC cluster and move hosts into the cluster. To enable EVC on an existing cluster, see Enable EVC on an Existing Cluster.

Other cluster features such as vSphere DRS and vSphere HA are fully compatible with EVC. You can enable these features when you create the cluster.

Prerequisites

Verify that the hosts you intend to add to the cluster meet the requirements listed in EVC Requirements for Hosts.

Procedure

1. Right-click a data center in the inventory and select **New Cluster**.
2. Type a name for the cluster.
3. Expand **EVC** and select a baseline CPU feature set from the **EVC mode** drop-down menu.

   Select a CPU vendor and EVC mode appropriate for the hosts that you intend to add to the cluster.
4. (Optional) Enable DRS.
5. (Optional) Enable vSphere HA.
6. Click **OK.**
7. Select a host to move into the cluster.

   If the host feature set is greater than the EVC mode that you enabled for the EVC cluster, power off all the virtual machines on the host, or use vMotion to migrate them to another host.

8 Move the host into the cluster.

   You can power on the virtual machines that are on the host, or migrate virtual machines into the cluster with vMotion. The virtual machines must meet CPU compatibility requirements for the EVC mode of the cluster.

You can now use vMotion to migrate virtual machines between different hosts in the cluster without encountering CPU incompatibility issues.

Enable EVC on an Existing Cluster

Enable EVC on an existing cluster to ensure vMotion CPU compatibility between the hosts in the cluster.

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 mode, you can change the EVC 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 http://kb.vmware.com/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. Select **VMware EVC**, and click **Edit**.
4. 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 **VMware EVC Mode** drop-down menu, select the baseline CPU feature set that you want to enable for the cluster.

   If you cannot select the EVC Mode, the Compatibility pane displays the reason, and the relevant hosts for each reason.
6. Click **OK**.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU 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 If the **EVC Mode** column is not visible, click the angle icon next to any column title and select **Show/Hide Columns > EVC Mode**.

The **EVC Mode** column shows the EVC modes of all virtual machines in the cluster or on the host.

Important For each virtual machine, the **EVC 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 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 Mode** column is defined in the following manner.

- When the virtual machine is powered on, the **EVC 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 Mode** column displays the EVC mode of the virtual machine.
Disabled	Enabled	Enabled. The **EVC Mode** column displays the EVC mode of the EVC cluster.

- When the virtual machine is powered off, the **EVC Mode** column displays the per-VM EVC mode. If per-VM EVC is disabled, the **EVC 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 Mode** column is defined in the following manner.

- When the virtual machine is powered on, the **EVC Mode** column displays the EVC mode of the parent host.
- When the virtual machine is powered off, the **EVC Mode** column is empty.

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.

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**.

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 in the vSphere Web Client

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.
Migrate virtual machine(s) to a specific datacenter	Move the virtual machine to a virtual data center, where you can assign policies to VMs.

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 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.

Option	Action
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.

6 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.

7 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**.

8 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.

9 On the Ready to complete page, review the details and click **Finish**.

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 .
- 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**.

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 in the vSphere Web Client

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 .
- 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**.

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 in the vSphere Web Client

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 .
- 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**.

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 Web Client, navigate to the host.
2. Click the **Configure** tab.
3. Select **Networking**, and click **VMkernel adapters**.
4. Click **Add host 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**.

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 Web Client, navigate to the host.
2. Click the **Configure** tab.
3. Select **Networking**, and click **VMkernel adapters**.
4. Click **Add host 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**.

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 13-2. Network Limits for Migration with vMotion

Operation	ESXi Version	Network Type	Maximum Cost
vMotion	5.0, 5.1, 5.5, 6.0	1GigE	4
vMotion	5.0, 5.1, 5.5, 6.0	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 1 against the source datastore and 1 against the destination datastore.

Table 13-3. 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	128	1
Storage vMotion	5.0, 5.1, 5.5, 6.0	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 13-4. 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	8	1
Storage vMotion	5.0, 5.1, 5.5, 6.0	2	4
vMotion Without Shared Storage	5.1, 5.5, 6.0	2	4
Other provisioning operations	5.0, 5.1, 5.5, 6.0	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

14

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.

The vSphere Client Developer Center provides tools for automation experts, devops engineers, and developers to find the resources to manage API structures and to capture vSphere Client actions to translate them into PowerCLI.

This chapter includes the following topics:

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 APIs available 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. From the home sidebar menu, click **Developer Center** and go to the **API Explorer** tab.
2. Using the **Select Endpoint** drop-down menu, select an endpoint from the environment.
3. Using the **Select API** drop-down menu, select an API. The listed APIs are the ones publicly provided by the existing API explorer on the vCenter Server Appliance.
4. (Optional) You can enter text into the filter text box to filter your results. For example, enter **`health`** to get a list of methods related to monitoring the health of the selected API.

5 To see detailed information about a method, click that method. Click **Execute** to invoke that method against the live environment.

   Code for the invoked method is produced in the response box.

6 (Optional) To copy the response code to your clipboard, click **Copy JSON**. You can download the response code by clicking **Download**.

Using Code Capture

Code Capture records user actions and translates them into executable code.

Code Capture gives you the ability to record actions taken in the vSphere Client and output them as usable PowerCLI code. You can then copy the code or download it as a script and use it in a PowerShell session to execute the task.

Note Only vCenter Server calls are recorded. Calls made on operations regarding roles, privileges, tags, content libraries, and storage policies are not recorded.

Record Actions Using Code Capture

You can use Code Capture to record actions taken in the vSphere Client to produce a PowerCLI code output.

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.

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 15

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.

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

A workflow is a series of actions and decisions that are automated to run sequentially after you initiate the workflow. Orchestrator provides a library of workflows that perform common management tasks according to best practices.

Basics of Workflows

Workflows consist of a schema, attributes, and 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 attributes and parameters are the variables that workflows use to transfer data. 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 Web 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 Web Client. You develop and manage workflows in the Orchestrator client. For more information about the Orchestrator client, see *Using the VMware vRealize Orchestrator Client*. For information about developing workflows, see *Developing with VMware vRealize Orchestrator*.

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 Web Client, the client loads the workflow presentation. You provide the input parameters of the workflow in the workflow presentation.

User Interaction

Some workflows require user intervention 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 Web 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 Web Client, you can perform the following tasks:

- Select a default 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 vSphere Web Client 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 Orchestrator server. Associate the workflows of the default 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 Web 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 both the vCenter Server and vSphere Web Client are 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 Web Client as a member of the Administrators group.
2. In the object navigator, click **vRealize Orchestrator**.
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**.

You successfully configured a default vRealize Orchestrator server in the vSphere Web 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 both the vCenter Server and vSphere Web Client are 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 thevSphere Web 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 both the vCenter Server and vSphere Web Client are 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 be able 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 from one vSphere Web Client to another by 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 both the vCenter Server and vSphere Web Client are 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 be able 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 both the vCenter Server and vSphere Web Client are 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 be able 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**.

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 Web Client.

You can perform some scheduling and running tasks on the Orchestrator workflows from the vRealize Orchestrator view in the vSphere Web 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 both the vCenter Server and vSphere Web Client are 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 both the vCenter Server and vSphere Web Client are 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 both the vCenter Server and vSphere Web Client are 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

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which both the vCenter Server and vSphere Web Client are 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 **Waiting for interaction**.

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

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which both the vCenter Server and vSphere Web Client are 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 **vRO Servers**.

   A list of the available vRealize Orchestrator servers appears.
3. Double-click a vRealize Orchestrator server.
4. Click **Categories**.
5. Double-click **Library**.

   Note **Library** is the default main workflow category. An Orchestrator server can have additional custom workflow categories.
6. Click **Categories**.

   A list of available workflow categories appears.
7. 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

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which both the vCenter Server and vSphere Web Client are 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 **Workflows**.
3. 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 both the vCenter Server and vSphere Web Client are 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 both the vCenter Server and vSphere Web Client are 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 both the vCenter Server and vSphere Web Client are 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 both the vCenter Server and vSphere Web Client are 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.

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 both the vCenter Server and vSphere Web Client are 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.

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 Web Client, make sure that you configure at least one running Orchestrator server to work with the same Single Sign-On instance to which both vCenter Server and vSphere Web Client are 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	Clones a Windows virtual machine performing the guest operating system customization. Configures one virtual network card and a local

single NIC and credential	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

16

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

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

17

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

These troubleshooting topics provide solutions to problems you might encounter when you use install vCenter Server on the Windows operating system or deploy the vCenter Server Appliance on a Linux system.

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 `C:\ProgramData\VMware\vCenterServer\logs` for Windows deployments or `/var/log/` for Linux deployments. Common logs are available in all implementations. Other logs are unique to certain deployment options (Management Node or Platform Services Controller).

Common Logs

The following logs are common to all deployments on Windows or Linux.

Table 17-1. Common Log Directories

Log Directory	Description
applmgmt	VMware Appliance Management Service
cloudvm	Logs for allotment and distribution of resources between services
cm	VMware Component Manager
firstboot	Location where first boot logs are stored

Log Directory	Description
rhttpproxy	Reverse Web Proxy
sca	VMware Service Control Agent
statsmonitor	Vmware Appliance Monitoring Service (Linux only)
vapi	VMware vAPI Endpoint
vmaffd	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 17-2. Management Node Log Directories

Log Directory	Description
autodeploy	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
invsvc	VMware Inventory Service
mbcs	VMware Message Bus Config Service
netdump	VMware vSphere ESXi Dump Collector
perfcharts	VMware Performance Charts
vmcam	VMware vSphere Authentication Proxy
vmdird	VMware Directory Service daemon
vmsyslog collector	vSphere Syslog Collector (Windows only)
vmware-sps	VMware vSphere Profile-Driven Storage Service
vmware-vpx	VMware VirtualCenter Server
vpostgres	vFabric Postgres database service
mbcs	VMware Message Bus Config Service
vsphere-client	VMware vSphere Web Client
vcha	VMware High Availability Service (Linux only)

Platform Services Controller Logs

You can examine the following logs if a Platform Services Controller node deployment is chosen.

Table 17-3. Platform Services Controller Node Log Directories

Log Directory	Description
cis-license	VMware Licensing Service
sso	VMware Secure Token Service
vmcad	VMware Certificate Authority daemon
vmdird	VMware Directory Service

For Platform Services Controller node deployments, additional runtime logs are located at `C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs`.

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.

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 the vSphere Web Client

The vSphere Web Client topics provide solutions to potential problems you might encounter when using the vSphere Web Client to manage vSphere components, including vCenter Single Sign-On and vCenter Server.

vCenter Server System Does Not Appear in vSphere Web Client Inventory

The vSphere Web Client does not display the vCenter Server systems that you expect to see in the inventory.

Problem

When you log in to the vSphere Web Client, the inventory appears to be empty or the vCenter Server system you expected to see does not appear.

Cause

In vSphere 5.1 and later, you log into the vSphere Web Client to view and manage multiple instances of vCenter Server. Any vCenter Server system on which you have permissions appears in the inventory when the server is registered with the same Component Manager as the vSphere Web Client.

Solution

- Log in to the vSphere Web Client as a user with permissions on the vCenter Server system.

  The vCenter Server system does not appear in the inventory if you do not have permissions on it. For example, if you log in as the vCenter Single Sign On administrator user, you might not have permissions on any vCenter Server system.

- Verify that the vCenter Server system is registered with the same Component Manager as the vSphere Web Client.

  The vSphere Web Client discovers only vCenter Server systems that are registered with the same Component Manager.

Unable to Start the Virtual Machine Console

When you attempt to open a virtual machine console from the vSphere Web Client, the console does not open.

Problem

When you attempt to open a virtual machine console from the vSphere Web Client, the console does not open. The following error message appears:

```
HTTP ERROR 404
Problem accessing /. Reason:
Not Found
```

Errors similar to the following appear in the `virgo-server.log` file:

```
[2012-10-03 18:34:19.170] [ERROR] Thread-40
System.err
                            2012-10-03
18:34:19.167:WARN:oejuc.AbstractLifeCycle:FAILED org.eclipse.jetty.server.Server@315b0333:
java.net.BindException: Address already in use
[2012-10-03 18:34:19.170] [ERROR] Thread-40 System.err java.net.BindException: Address already in use
```

Cause

Another application or process is using port 9443, the default port used by the HTML5 virtual machine console.

Solution

- Edit the `webclient.properties` file to add the line `html.console.port=`*port*, where *port* is the new port number.

  The `webclient.properties` file is located in one of the following locations, depending on the operating system on the virtual machine on which the vSphere Web Client is installed:

Windows 2008	`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\`
vCenter Server Appliance	`/etc/vmware/vsphere-client/`

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.

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.

Log into the host as the root user and reconnect the host to vCenter Server.

Cannot Configure vSphere HA When Using Custom SSL Certificates

After you install custom SSL certificates, attempts to enable vSphere High Availability (HA) fail.

Problem

When you attempt to enable vSphere HA on a host with custom SSL certificates installed, the following error message appears: `vSphere HA cannot be configured on this host because its SSL thumbprint has not been verified.`

Cause

When you add a host to vCenter Server, and vCenter Server already trusts the host's SSL certificate, `VPX_HOST.EXPECTED_SSL_THUMBPRINT` is not populated in the vCenter Server database. vSphere HA obtains the host's SSL thumbprint from this field in the database. Without the thumbprint, you cannot enable vSphere HA.

Solution

1. In the vSphere Web Client, disconnect the host that has custom SSL certificates installed.
2. Reconnect the host to vCenter Server.
3. Accept the host's SSL certificate.
4. Enable vSphere HA on the host.

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 master 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 master 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.

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 master host or to connect to the master 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.

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 master host or a slave 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.

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 master host and lock a datastore. Locking a datastore prevents the valid cluster master 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.

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 master 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.

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 master hosts that are responsible for them, vSphere HA's ability to restart the virtual machines after a failure is affected. First, each master 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 master 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.

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 master 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 master 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 master 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.

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.

Set the vCenter Server advanced option config.vpxd.das.electionWaitTimeSec to value=240. Once this change is made, the time outs do not occur.

Troubleshooting vSphere Auto Deploy

The vSphere Auto Deploy troubleshooting topics offer solutions for situations when provisioning hosts with vSphere Auto Deploy does not work as expected.

vSphere Auto Deploy TFTP Timeout Error at Boot Time

A TFTP Timeout error message appears when a host provisioned with vSphere Auto Deploy boots. The text of the message depends on the BIOS.

Problem

A TFTP Timeout error message appears when a host provisioned with vSphere Auto Deploy boots. The text of the message depends on the BIOS.

Cause

The TFTP server is down or unreachable.

- Ensure that your TFTP service is running and reachable by the host that you are trying to boot.
- To view the diagnostic logs for details on the present error, see your TFTP service documentation.

vSphere Auto Deploy Host Boots with Wrong Configuration

A host is booting with a different ESXi image, host profile, or folder location than the one specified in the rules.

Problem

A host is booting with a different ESXi image profile or configuration than the image profile or configuration that the rules specify. For example, you change the rules to assign a different image profile, but the host still uses the old image profile.

Cause

After the host has been added to a vCenter Server system, the boot configuration is determined by the vCenter Server system. The vCenter Server system associates an image profile, host profile, or folder location with the host.

Solution

- Use the `Test-DeployRuleSetCompliance` and `Repair-DeployRuleSetCompliance` vSphere PowerCLI cmdlets to reevalute the rules and to associate the correct image profile, host profile, or folder location with the host.

Host Is Not Redirected to vSphere Auto Deploy Server

During boot, a host that you want to provision with vSphere Auto Deploy loads iPXE. The host is not redirected to the vSphere Auto Deploy server.

Problem

During boot, a host that you want to provision with vSphere Auto Deploy loads iPXE. The host is not redirected to the vSphere Auto Deploy server.

Cause

The `tramp` file that is included in the TFTP ZIP file has the wrong IP address for the vSphere Auto Deploy server.

Solution

- Correct the IP address of the vSphere Auto Deploy server in the `tramp` file, as explained in the *vSphere Installation and Setup* documentation.

Package Warning Message When You Assign an Image Profile to a vSphere Auto Deploy Host

When you run a vSphere PowerCLI cmdlet that assigns an image profile that is not vSphere Auto Deploy ready, a warning message appears.

Problem

When you write or modify rules to assign an image profile to one or more hosts, the following error results:

```
Warning: Image Profile <name-here> contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.
```

Cause

Each VIB in an image profile has a `stateless-ready` flag that indicates that the VIB is meant for use with vSphere Auto Deploy. You get the error if you attempt to write a vSphere Auto Deploy rule that uses an image profile in which one or more VIBs have that flag set to FALSE.

Note You can use hosts provisioned with vSphere Auto Deploy that include VIBs that are not stateless ready without problems. However booting with an image profile that includes VIBs that are not stateless ready is treated like a fresh install. Each time you boot the host, you lose any configuration data that would otherwise be available across reboots for hosts provisioned with vSphere Auto Deploy.

Solution

1. Use vSphere ESXi Image Builder cmdlets in a vSphere PowerCLI session to view the VIBs in the image profile.
2. Remove any VIBs that are not stateless-ready.
3. Rerun the vSphere Auto Deploy cmdlet.

vSphere Auto Deploy Host with a Built-In USB Flash Drive Does Not Send Coredumps to Local Disk

If your vSphere Auto Deploy host has a built-in USB flash drive, and an error results in a coredump, the coredump is lost. Set up your system to use ESXi Dump Collector to store coredumps on a networked host.

Problem

If your vSphere Auto Deploy host has a built-in USB Flash, and if it encounters an error that results in a coredump, the coredump is not sent to the local disk.

Solution

1. Install ESXi Dump Collector on a system of your choice.

   ESXi Dump Collector is included with the vCenter Server installer.

2. Use ESXCLI to configure the host to use ESXi Dump Collector.

   ```
   esxcli conn_options system coredump network set IP-addr,port
   esxcli system coredump network set -e true
   ```

3. Use ESXCLI to disable local coredump partitions.

   ```
   esxcli conn_options system coredump partition set -e false
   ```

vSphere Auto Deploy Host Reboots After Five Minutes

A vSphere Auto Deploy host boots and displays iPXE information, but reboots after five minutes.

Problem

A host to be provisioned with vSphere Auto Deploy boots from iPXE and displays iPXE information on the console. However, after five minutes, the host displays the following message to the console and reboots.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

The host might also display the following details:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

The console then displays the host's machine attributes including vendor, serial number, IP address, and so on.

Cause

No image profile is currently associated with this host.

You can assign an image profile to the host by running the `Apply-EsxImageProfile` cmdlet, or by creating the following rule:

1 Run the `New-DeployRule` cmdlet to create a rule that includes a pattern that matches the host with an image profile.

2 Run the `Add-DeployRule` cmdlet to add the rule to a ruleset.

3 Run the `Test-DeployRuleSetCompliance` cmdlet and use the output of that cmdlet as the input to the `Repair-DeployRuleSetCompliance` cmdlet.

vSphere Auto Deploy Host Cannot Contact TFTP Server

The host that you provision with vSphere Auto Deploy cannot contact the TFTP server.

Problem

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host performs a network boot and is assigned a DHCP address by the DHCP server, but the host cannot contact the TFTP server.

Cause

The TFTP server might have stopped running, or a firewall might block the TFTP port.

- If you installed the WinAgents TFTP server, open the WinAgents TFTP management console and verify that the service is running. If the service is running, check the Windows firewall's inbound rules to make sure the TFTP port is not blocked. Turn off the firewall temporarily to see whether the firewall is the problem.
- For all other TFTP servers, see the server documentation for debugging procedures.

vSphere Auto Deploy Host Cannot Retrieve ESXi Image from vSphere Auto Deploy Server

The host that you provision with vSphere Auto Deploy stops at the iPXE boot screen.

Problem

When you attempt to boot a host provisioned with vSphere Auto Deploy, the boot process stops at the iPXE boot screen and the status message indicates that the host is attempting to get the ESXi image from the vSphere Auto Deploy server.

Cause

The vSphere Auto Deploy service might be stopped or the vSphere Auto Deploy server might be unaccessible.

Solution

1. Log in to the system on which you installed the vSphere Auto Deploy server.
2. Check that the vSphere Auto Deploy server is running.
   a. Click **Start > Settings > Control Panel > Administrative Tools**.
   b. Double-click **Services** to open the Services Management panel.
   c. In the Services field, look for the VMware vSphere Auto Deploy Waiter service and restart the service if it is not running.
3. Open a Web browser, enter the following URL, and check whether the vSphere Auto Deploy server is accessible.

   https://*Auto_Deploy_Server_IP_Address*:*Auto_Deploy_Server_Port*/vmw/rdb

   Note Use this address only to check whether the server is accessible.
4. If the server is not accessible, a firewall problem is likely.
   a. Try setting up permissive TCP Inbound rules for the vSphere Auto Deploy server port.

      The port is 6501 unless you specified a different port during installation.
   b. As a last resort, disable the firewall temporarily and enable it again after you verified whether it blocked the traffic. Do not disable the firewall on production environments.

      To disable the firewall, run `netsh firewall set opmode disable`. To enable the firewall, run `netsh firewall set opmode enable`.

vSphere Auto Deploy Host Does Not Get a DHCP Assigned Address

The host you provision with vSphere Auto Deploy fails to get a DHCP Address.

Problem

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host performs a network boot but is not assigned a DHCP address. The vSphere Auto Deploy server cannot provision the host with the image profile.

Cause

You might have a problem with the DHCP service or with the firewall setup.

Solution

1. Check that the DHCP server service is running on the Windows system on which the DHCP server is set up to provision hosts.
   a. Click **Start > Settings > Control Panel > Administrative Tools**.
   b. Double-click **Services** to open the Services Management panel.
   c. In the Services field, look for the DHCP server service and restart the service if it is not running.

2 If the DHCP server is running, recheck the DHCP scope and the DHCP reservations that you configured for your target hosts.

   If the DHCP scope and reservations are configured correctly, the problem most likely involves the firewall.

3 As a temporary workaround, turn off the firewall to see whether that resolves the problem.

   a Open the command prompt by clicking **Start > Program > Accessories > Command prompt**.

   b Type the following command to temporarily turn off the firewall. Do not turn off the firewall in a production environment.

   ```
   netsh firewall set opmode disable
   ```

   c Attempt to provision the host with vSphere Auto Deploy.

   d Type the following command to turn the firewall back on.

   ```
   netsh firewall set opmode enable
   ```

4 Set up rules to allow DHCP network traffic to the target hosts.

   See the firewall documentation for DHCP and for the Windows system on which the DHCP server is running for details.

vSphere Auto Deploy Host Does Not Network Boot

The host you provision with vSphere Auto Deploy comes up but does not network boot.

Problem

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host does not start the network boot process.

Cause

You did not enable your host for network boot.

Solution

1 Reboot the host and follow the on-screen instructions to access the BIOS configuration.

2 In the BIOS configuration, enable Network Boot in the Boot Device configuration.

Recovering from Database Corruption on the vSphere Auto Deploy Server

In some situations, you might have a problem with the vSphere Auto Deploy database. The most efficient recovery option is to replace the existing database file with the most recent backup.

Problem

When you use vSphere Auto Deploy to provision the ESXi hosts in your environment, you might encounter a problem with the vSphere Auto Deploy database.

Important This is a rare problem. Follow all other vSphere Auto Deploy troubleshooting strategies before you replace the current database file. Rules or associations that you created since the backup you choose are lost.

Cause

This problem happens only with hosts that are provisioned with vSphere Auto Deploy.

Solution

1. Stop the vSphere Auto Deploy server service.
2. Find the vSphere Auto Deploy log by going to the vSphere Auto Deploy page in the vSphere Web Client.
3. Check the logs for the following message:

   `DatabaseError: database disk image is malformed.`

   If you see the message, replace the existing database with the most recent backup.
4. Go to the vSphere Auto Deploy data directory.

Operating System	File Location
vCenter Server appliance	`/var/lib/rbd`
Microsoft Windows	`%VMWARE_DATA_DIR%\autodeploy\Data`

   The directory contains a file named `db`, and backup files named `db-yyy-mm-dd`.
5. Rename the current `db` file.

   VMware Support might ask for that file if you call for assistance.
6. Rename the most recent backup to `db`.
7. Restart the vSphere Auto Deploy server service.
8. If the message still appears in the log, repeat the steps to use the next recent backup until vSphere Auto Deploy works without database errors.

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.

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.

Active Directory Rule Set Error Causes Host Profile Compliance Failure

Applying a host profile that specifies an Active Directory domain to join causes a compliance failure.

Problem

When you apply a host profile that specifies an Active Directory domain to join, but you do not enable the **activeDirectoryAll** rule set in the firewall configuration, a compliance failure occurs. The vSphere Web Client displays the error message `Failures against the host profile: Ruleset activedirectoryAll does not match the specification`. The compliance failure also occurs when you apply a host profile to leave an Active Directory domain, but you do not disable the **activeDirectoryAll** rule set in the host profile.

Cause

Active Directory requires the **activeDirectoryAll** firewall rule set. You must enable the rule set in the firewall configuration. If you omit this setting, the system adds the necessary firewall rules when the host joins the domain, but the host will be noncompliant because of the mismatch in firewall rules. The host will also be noncompliant if you remove it from the domain without disabling the Active Directory rule set.

Solution

1 Browse to the host profile in the vSphere Web Client.

   To find a host profile, click **Policies and Profiles > Host Profiles** on the vSphere Web Client Home page.

2 Right-click the host profile and select **Edit Settings**.

3 Click **Next**.

4 Select **Security and Services > Firewall Configuration > Firewall configuration > Ruleset Configuration**.

5 Ensure that **activeDirectoryAll** is selected.

6 In the right panel, select the **Flag indicating whether ruleset should be enabled** check box.

Deselect the check box if the host is leaving the domain.

7 Click **Next**, and then click **Finish** to complete the change to the host profile.

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.

- 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.

- 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.

Table 17-4. 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.

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.