vCloud DirectorTenant Portal Guide

04 OCT 2018

vCloud Director 9.5

vmware®

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

https://docs.vmware.com/

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

Table of Contents

vCloud Director Tenant Portal Guide

The *VMware vCloud Director Tenant Portal Guide* provides information about how to use the VMware vCloud Director tenant portal. In this release, you use the tenant portal to administrate your organization, create and configure virtual machines, vApps, and networks within vApps.
With the vCloud Director tenant portal, you can also create and manage catalogs, vApp and VDC templates, and create and manage cross-virtual data center networks.

Intended Audience

This guide is intended for anyone who wants to use the capabilities of the vCloud Director the tenant portal. The information is written primarily for **organization administrators** who use the tenant portal to administer their organization, manage virtual machines, vApps, networks, and so on.

Related Documentation

See the *vCloud Director User's Guide* for information about the features and capabilities available to an

organization administrator using the vCloud Director Web console instead of the vCloud Director tenant portal.

VMware Technical Publications Glossary

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

Updated Information

This *vCloud Director Tenant Portal Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *vCloud Director Tenant Portal Guide*.

Revision	Description
28 NOV 2018	■ Added information about the IPv6 support in this release. ■ Updated Using the vCloud Director Tenant Portal to add a reference about customizing the portal. ■ Updated topic Upgrade the Virtual Hardware Version for a Virtual Machine to provide information about the supported virtual hardware versions.
05 NOV 2018	■ Updated the rights in Predefined Roles and Their Rights.
04 OCT 2018	Initial release.

Getting Started with the vCloud Director Tenant Portal

1

When you log into the tenant portal, there are a number of tasks you can complete, from creating virtual machines and vApps, to setting up advanced networking configuration and running vRealize Orchestrator workflows.

This chapter includes the following topics:

Understanding VMware vCloud Director

VMware® vCloud Director provides role-based access to a web-based tenant portal that allows the members of an organization to interact with the organization's resources to create and work with vApps and virtual machines.

Before you can access your organization, a vCloud Director **system administrator** must create the organization, assign it resources, and provide the URL to access the tenant portal. Each organization includes one or more **organization administrators**, who finish setting up the organization by adding members and setting policies and preferences. After the organization is set up, non-administrator users can log in to create, use, and manage virtual machines and vApps.

Organizations

An organization is a unit of administration for a collection of users, groups, and computing resources. Users authenticate at the organization level, supplying credentials established by an **organization administrator** when the user was created or imported. **System administrators** create and provision organizations, while **organization administrators** manage organization users, groups, and catalogs.

Users and Groups

An organization can contain an arbitrary number of users and groups. Users can be created locally by the organization administrator or imported from a directory service such as LDAP or vCenter Single Sign-On. Groups must be imported from the directory service. Permissions within an organization are controlled through the assignment of rights and roles to users and groups.

Virtual Data Centers

An organization virtual data center provides resources to an organization. Virtual data centers provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual CD and DVD media. An organization can have multiple virtual data centers.

Organization Virtual Data Center Networks

An organization virtual data center network is contained within a vCloud Director organization virtual data center and is available to all the vApps in the organization. An organization virtual data center network allows vApps within an organization to communicate with each other. An organization virtual data center network can be connected to an external network or isolated and internal to the organization. Only **system administrators** can create organization virtual data center networks, but **organization administrators** can manage organization virtual data center networks, including the network services they provide.

vApp Networks

A vApp network is contained within a vApp and allows virtual machines in the vApp to communicate with each other. You can connect a vApp network to an organization virtual data center network to allow the vApp to communicate with other vApps in the organization and outside of the organization, if the organization virtual data center network is connected to an external network.

Catalogs

Organizations use catalogs to store vApp templates and media files. The members of an organization that have access to a catalog can use its vApp templates and media files to create their own vApps. **Organization administrators** can copy items from public catalogs to their organization catalog.

Log In to the vCloud Director Tenant Portal

You can access the vCloud Director tenant portal by using a URL that is specific to your organization.

Contact your **organization administrator** if you do not know the tenant portal organization URL. See the *vCloud Director Release Notes* for information about supported browsers and configurations.

Procedure

1 In a Web browser, navigate to the tenant portal URL of your organization.

For example, *https://vcloud.example.com/tenant/myOrg*.

2 Enter your user name and password, and click **Log In**.

vCloud Director Tenant Portal Roles and Rights

vCloud Director includes a preconfigured set of user roles and their rights. The roles that are able to access the vCloud Director tenant portal are the roles created by default in any organization or other roles that are created by the organization administrator.

Users who are assigned the following organization roles can access the tenant portal. The items they see and the actions they can perform depend on the rights that are associated with a particular role.

- **Organization Administrator**
- **Catalog Author**
- **vApp Author**
- **vApp User**
- **Console Access Only**

For information about the predefined roles and their rights, see Predefined Roles and Their Rights.

Using the vCloud Director Tenant Portal

If you have more than one virtual data center, when you log in to the vCloud Director tenant portal, you are navigated to the **Virtual Datacenters** dashboard screen. If you have only one virtual data center, when you log in to the vCloud Director tenant portal, you are directly navigated to the data center.

The **Virtual Datacenters** dashboard screen is part of the vCloud Director multisite feature that makes it possible for tenants to see their geographically distributed cloud environment as a single entity. For more information about multisite, see Working with Multiple Sites.

The dashboard is a unified view of the vCloud Director virtual data centers and sites not only in a single organization. In a multi-cell and multi-organization environment, you can also see the virtual data centers for all other associated organizations.

Note Depending on their rights, tenant users can see all member sites of an organization or only a subset of sites.

The information about the organization is displayed on top in the summary ribbon.

If you log in as an **organization administrator**, you can see:

- The number of sites, organizations, and virtual data centers

- Total number of running vApps and virtual machines
- Used hardware resources, such as CPU, memory, and storage

The virtual data centers display in a card view. Each card contains information about the organization to which the virtual center belongs, the number of vApps, the total number of virtual machines and the number of virtual machines that are in a running state. The card also shows the available CPU, memory, and storage capacity for the data center and displays real-time metrics about the current allocations and reservations of resources.

From the main menu ☰), you can navigate to the different menu items.

Menu Item	Description
Datacenters	Navigates you to the **Virtual Datacenters** screen that displays the virtual data centers within the organization.
Content Libraries	Navigates you to a consolidated view for vApp templates, catalogs, media, and other types of files. You use these templates and files to deploy virtual machines or vApps.
Administration	Navigates you to the multisite management screen where **organization administrators** can create a trust association with another organization.
Tasks	Navigates you to the **Tasks** screen that displays the tasks reported by vCloud Director.
Events	Navigates you to the **Events** screen that displays the events reported by vCloud Director.
Operations	Navigates you to the **Service Library** screen. The **Service Library** contains groups of vCloud Director components, for which you can run vRealize Orchestrator workflows.

You can customize your vCloud Director Tenant Portal by using the Branding vCloud OpenAPIs. For information about using the vCloud OpenAPI, see the *Getting Started vCloud OpenAPI* document at https://code.vmware.com.

View Tasks

From the tenant portal, you can view the list of recent tasks, together with their details and status. In addition, you can also see the list of all tasks.

By default, the **Recent Tasks** panel is displayed at the bottom of the tenant portal and contains a list of the tasks that have been recently run. When you start an operation, for example to create a virtual machine, the task is displayed in the panel. In case you minimize the **Recent Tasks** panel, you still see the number of running or failed recent tasks. You can always open the **Recent Tasks** panel again by clicking the double arrows.

The tasks view lists all tasks and shows when tasks were run, and whether they were successfully completed. This view is the first step for troubleshooting problems in your environment. The tasks view contains long running operations, such as virtual machine or vApp creation.

Procedure

1. From the main menu ☰), select **Tasks**, or click **More tasks** under the **Recent Tasks** panel.

   The list of all tasks displays, together with the time the task was run, and the status of the task.

2 Click the editor icon () to change the details you want to view about the tasks.

3 (Optional) To view the task details, click the name of the task.

The task details include information such as the reason for the failure, when the task has failed, and so on.

Detail	Description
Operation	Name of the performed operation.
Job ID	ID of the task.
Type	The object on which the task was performed. For example, if you created a virtual machine, the type is vm.
Organization	Organization name.
Status	Status of the task, such as Succeeded, Running, or Failed.
Initiator	User who started the operation.
Start time	Date and time when the operation started.
Completion time	Date and time when the operation succeeded or failed.

Detail	Description
Service namespace	Service name, such as *com.vmware.vcloud*.
Details	Reason for the failure of the task. For example, if you try to create a snapshot of a virtual machine, and the operation fails, because the storage is insufficient, the task details are of the type: The requested operation will exceed the VDC's storage quota: storage policy " " has* 8,693 MB remaining, requested 41,472 MB.

Stop a Task in Progress

If you accidentally start an operation before applying or reviewing all necessary settings, you can stop the task in progress.

By default, the **Recent Tasks** panel is displayed at the bottom of the portal. When you start an operation, for example to create a virtual machine, the task is displayed in the panel.

Prerequisites

The **Recent Tasks** panel must be open.

Procedure

1. Start a long-running operation.

   Long-running operations are operations such as creating a virtual machine or a vApp, power operations performed on virtual machines and vApps, and so on.

2. In the **Recent Tasks** panel, click the **Cancel** icon ( ).
3. In the **Cancel Task** dialog box, confirm that you want to cancel the task by clicking **OK**.

The operation stops.

View Events

From the portal, you can view the list of all events, as well as their details and status.

The events view is a way to view the status of the events in your portal. The view shows when the events happened, and whether they were successful. The events view contains one-time occurrences, such as user logins and object creation, or deletion.

Procedure

1. From the main menu), select **Events**.

   The list of all events displays, along with the time the event happened and the status of the event.

2. Click the editor icon ( ) to change the details you want to view about the events.

3 (Optional) Click an event to view the event details.

Detail	Description
Event	Name of the event. For example, if you modify a vApp to include virtual machines in it, the event that starts the whole operation is *Task 'Modify vApp' start*.
Event ID	ID of the task.
Type	The object on which the task was performed. For example, if you created a virtual machine, the type is *vm*.
Target	Target object of the event. For example, when you modify a vApp to include virtual machines in it, the target of the *Task 'Modify vApp' start* event is *vdcUpdateVapp*.
Status	Status of the event, such as Succeeded or Failed.
Service namespace	Service name, such as *com.vmware.vcloud*.
Organization	Name of the organization.
Owner	User who triggered the event.
Time of occurrence	Date and time when the event occurred.

Working with Virtual Machines

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine consists of a set of specification and configuration files, and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware but are more portable, more secure, and easier to manage.

In addition to the operations that you can run on a physical machine, vCloud Director virtual machines support virtual infrastructure operations, such as taking a snapshot of virtual machine state, and moving a virtual machine from one host to another.

Starting with vCloud Director 9.5, virtual machines support IPv6 connectivity. You can assign IPv6 addresses to virtual machines connected to IPv6 networks.

Important All steps for working with virtual machines are documented from the card view, assuming that you have more than one virtual data center. Completing the same procedures from the grid view is also possible, but the steps might slightly vary.

This chapter includes the following topics:

- Monitor Virtual Machines
- Working with Snapshots
- Renew a Virtual Machine Lease
- Delete a Virtual Machine

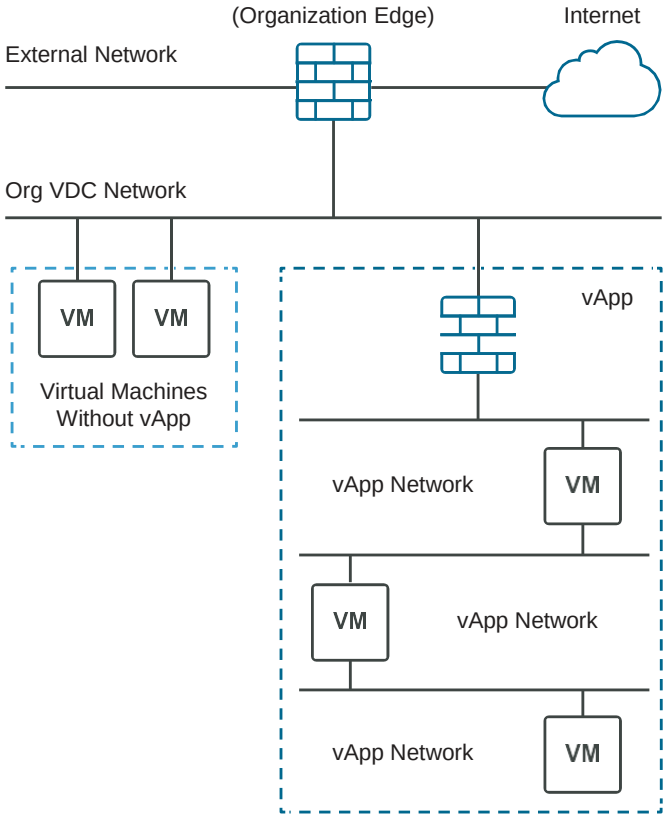
Virtual Machine Architecture

A virtual machine can exist as a standalone machine or it can exist within a vApp.

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine consists of a set of specification and configuration files, and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware but are more portable, more secure, and easier to manage. Virtual machines can be standalone, or they can exist within a vApp. A vApp is a compound object composed of one or more virtual machines, as well as one or more networks.

The following figure shows the different options when creating a virtual machine. You can create a standalone virtual machine or a virtual machine within a vApp. The standalone virtual machine is directly connected to the organization virtual data center. You can also create a virtual machine within a vApp. By creating a virtual machine inside of a vApp, you can group together multiple virtual machines and their associated networks. vApps allow you to build complex applications, and save them to a catalog for future use.

Figure 2-1. Virtual Machines are Standalone or within a vApp



View and Edit Virtual Machines

You can view virtual machines that are standalone or part of a vApp. You can view virtual machines in a grid view or in a card view.

Procedure

1. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
2. To view the virtual machines in a grid view, click  . Or to view them in a card view, click  .

   The list of virtual machines displays in a grid view or as a list of cards.

3 (Optional) Configure the grid view to contain details you want to see about each virtual machine.

   a From the grid view, click the **Grid editor** icon ().

   b Select the virtual machine details you want to include in the grid view by selecting the check box next to each detail you want to see.

   Details include information about the hardware version, VMware Tools, memory, and so on.

   c To save your changes, click **OK**.

   The selected details appear as columns for each virtual machine.

4 (Optional) From the grid view, click  on the left of a virtual machine, to display the actions you can take for the selected virtual machine.

   For example, you can shut down a virtual machine.

5 To access the interface for the guest operating system of the virtual machine, click the desktop icon in the upper right corner of the card view.

Create a New Standalone Virtual Machine

You can create a new standalone virtual machine.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 Click **Create VM**.

4 Enter the name and the computer name for the virtual machine.

   Important The computer name can contain only alphanumeric characters and cannot consist of digits only.

5 Select whether you want the virtual machine to power on right after it is created.

6 (Optional) Enter a meaningful description.

7 Select how you want to deploy the virtual machine.

Option	Action
New	You deploy a new virtual machine with customizable settings. a Select an Operating System family and Operating System. b (Optional) Select a Boot image. c Select the size of the virtual machine or click **Customize** to enter the compute, memory, and storage settings manually. The size of the virtual machine can be as small, medium, or large. d Specify the network settings for the virtual machine, such as network, IP mode, IP address, and primary NIC.
From Template	You deploy a virtual machine from a template that you select from the templates catalog.

8 Click **OK** to save the settings of the virtual machine and to start the creation process.

You can see the card of the virtual machine in the catalog. Until the virtual machine is created, its state is displayed as Busy.

Opening a Virtual Machine Console

Accessing your virtual machine console allows you to view information about the virtual machine, work with the guest operating system, and perform operations that affect the guest operating system.

Prerequisites

The virtual machine is powered on.

Install VMware Remote Console on a Client

VMware Remote Console provides an embedded user-guest interaction in all virtual machines that are provisioned and managed by vCloud Director. This section details the tasks required to install VMware Remote Console on Windows, Apple OS X, and Linux.

Prerequisites

This operation requires the rights included in the predefined **vApp User** role or an equivalent set of rights.

Procedure

1 Download the installer.

- Navigate to the Evolve IP's VMware Remote Console (VMRC) download page, and select the link: https://sync.evolveip.net:510/shares/file/1980521dabb580/

- On the **Virtual Datacenters** dashboard screen in the vCloud Director tenant portal, click the card of the virtual datacenter that you want to explore. Select a virtual machine, and click **More > Download VMRC**.

2 Run your platform installation.

- Windows

  Double click the .msi installer and follow the prompts.

- Linux

  With root privileges, run the .bundle installer and follow the prompts.

- Mac

  Double click the .dmg to open it, then double-click the VMware Remote Console icon inside to copy to the Applications folder.

After installation, VMware Remote Console opens when you click Uniform Resource Identifiers (URIs) that begin with the vmrc:// scheme. VMware Workstation, Player, and Fusion also handle the vmrc:// URI scheme.

Open a Virtual Machine Remote Console

You can open a virtual machine console using VMware Remote Console through the vCloud Director Tenant Portal.

Prerequisites

- Verify that VMware Remote Console is installed on your local system.
- Make sure that the selected virtual machine is in a powered-on state.
- This operation requires the rights included in the predefined **vApp User** role or an equivalent set of rights.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine, select **Launch VM Remote Console**.

Note If you do not have the VMware Remote Console installed, a pop-up window prompts you to either install VMware Remote Console or use the Web console.

The virtual machine console opens as an external virtual remote console.

Note When you connect to a vCloud Director virtual machine by using VMware Remote Console, you are limited to console interaction only (sending Ctrl+Alt+Del). You cannot perform device operations, power operations, or settings management.

Open a Web Console

You can connect to the console of a virtual machine even if you do not have VMware Remote Console installed on your local system.

Prerequisites

- Verify that the virtual machine is powered on.
- This operation requires the rights included in the predefined **vApp User** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **More** menu of the virtual machine, select **Launch Web Console**.

The virtual machine console opens in a new browser tab by using the VMware HTML Console SDK.

What to do next

Click anywhere inside the console window to start using your mouse, keyboard, and other input devices in the console.

Note For information about supported international keyboards, see the VMware HTML Console SDK Documentation at https://www.vmware.com/support/developer/html-console/.

Performing Power Operations on Virtual Machines

You can perform power operations on virtual machines, such as power on or off a virtual machine, suspending or resetting a virtual machine or shutting down the guest Operating System of a virtual machine.

Power On a Virtual Machine

Powering on a virtual machine is the equivalent of powering on a physical machine.

You cannot power on a virtual machine that has guest customization enabled unless the virtual machine has a current version of VMware Tools installed.

Prerequisites

The virtual machine is powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **Power** menu of the virtual machine you want to start, select **Power On**.

A powered-on virtual machine displays a Powered on status in green.

Power Off a Virtual Machine

Powering off a virtual machine is the equivalent of powering off a physical machine.

Prerequisites

The virtual machine is powered on.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **Power** menu of the virtual machine you want to power off, select **Power Off**.

A powered-off virtual machine displays a Powered off status in red.

Shut Down a Guest Operating System

Shutting down the guest operating system of a virtual machine is the equivalent of powering off a physical machine.

Prerequisites

The virtual machine and guest operating system must be powered on.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **Power** menu of the virtual machine, select **Shut Down Guest OS**.

The guest OS is shut down.

Reset a Virtual Machine

Resetting a virtual machine clears state (memory, cache, and so on), but the virtual machine continues to run. Resetting a virtual machine is the equivalent of pushing the reset button of a physical machine. It initiates a hard reset of the operating system without changing the power state of the virtual machine.

Prerequisites

Your virtual machine is powered on.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **Power** menu of the virtual machine you want to reset, select **Reset**.

The state clears for the virtual machine.

Suspend a Virtual Machine

Suspending a virtual machine preserves its current state by writing the memory to disk.

The suspend and resume feature is useful when you want to save the current state of your virtual machine and continue work later from the same state.

Prerequisites

The virtual machine is powered on.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **Power** menu of the virtual machine you want to suspend, select **Suspend**.

The virtual machine is suspended, but its state is preserved.

Discard the Suspended State of a Virtual Machine

If a virtual machine is in a suspended state and you no longer need to resume the use of the machine, you can discard the suspended state. Discarding the suspended state removes the saved memory and returns the machine to a powered-off state.

Prerequisites

A virtual machine that is suspended.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list of virtual machines in a grid view. Select the virtual machine for which you want to discard the state.
3. Click the list bar () on the left of the suspended virtual machine and select **Discard suspended state**.

The state is discarded, and the virtual machine is powered off.

Install VMware Tools in a Virtual Machine

vCloud Director depends on VMware Tools to customize the guest OS.

VMware Tools improves management and performance of the virtual machine by replacing generic operating system drivers with VMware drivers tuned for virtual hardware. You install VMware Tools into the guest operating system. Although the guest operating system can run without VMware Tools, you lose important features and convenience.

Prerequisites

- The virtual machine must be powered on.
- If your newly created virtual machine has no guest operating system, you must install it before you can install VMware Tools.
- Guest customization must be disabled prior to installing VMware Tools.
- If the version of VMware Tools is earlier than 7299 in a virtual machine in your vApp, you must upgrade it.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine in which you want to install VMware Tools, select **Install VMware Tools**.

VMware Tools is installed on the target guest operating system. If there is an error during installation, an error message displays. You can also view the progress of the installation operation in the **Tasks** window.

4 Open the Web console of the virtual machine by clicking **More > Launch Web Console**.

5 Follow the instructions on the VMware Knowledge Base Article 1014294 to configure the VMware Tools for your particular operating system.

VMware Tools is installed and configured on the guest operating system.

Upgrade the Virtual Hardware Version for a Virtual Machine

You can upgrade the virtual hardware version for a virtual machine. Later virtual hardware versions support more features.

You cannot downgrade the hardware version of the virtual machines in a vApp.

VMware vCloud Directorsupports hardware versions depending on the resources backing the organization VDC, which depends on the latest supported virtual hardware in the backing provider VDC. The **Organization Administrator** or the **System Arministrator** can set the hardware version to an earlier one. The vCloud Director tenant portal dynamically sets the list of selectable virtual hardware versions based on the backing hardware of the organization VDC or the provider VDC.

For information about hardware features available with virtual machine compatibility settings, see *vSphereVirtual Machine Administration Guide*.

For information about the latest version for the VMware product that you are using, see https://kb.vmware.com/s/article/1003746.

Prerequisites

- Stop the vApp.
- Verify that the latest version of VMware tools is installed on the virtual machines.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine you want to upgrade, select **Upgrade Virtual Hardware Version**.

4 Click **OK**.

The virtual machine is upgraded to the latest version.

Edit Virtual Machine Properties

You can edit the properties of a virtual machine, including the virtual machine name and description, hardware and network settings, guest OS settings, and so on.

Change the General Properties of a Virtual Machine

You can review and change the name, description, and other general properties of a virtual machine.

Prerequisites

Changing properties such as operating system, requires that the machine is powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 In the card of the virtual machine you want to edit, click **Details**.

4 The list of properties that you can view or edit under **General** expands by default.

Option	Description
Virtual Machine Name	Edit the name of the virtual machine. You can edit this property while the virtual machine is powered on.
Computer Name	Edit the computer and host name set in the guest operating system that identifies the virtual machine on a network. This field is restricted to 15 characters because of a Windows OS limitation on computer names. You can edit this property while the virtual machine is powered on.
Description	Type an optional description of the virtual machine. You can edit this property while the virtual machine is powered on.
Operating System Family	Select an operating system family from the drop-down menu. You can edit this property while the virtual machine is powered off. In addition, you cannot edit this property if an operating system is already present on the virtual machine.
Operating System	Select an operating system from the drop-down menu. You can edit this property while the virtual machine is powered off. In addition, you cannot edit this property if an operating system is already present on the virtual machine.

Option	Description
Boot Delay	The time between when you power on the virtual machine and when it exits the BIOS and launches the guest operating system software can be short. You can change the boot delay to provide more time. Select the time in milliseconds to delay the boot operation.
Storage Policy	Select a storage policy for the virtual machine to use from the drop-down menu. You can edit this property while the virtual machine is powered on.
Virtual Data Center	View the name of the virtual data center.
VMware Tools	View whether VMware Tools is installed on the virtual machine.
Virtual Hardware Version	View the virtual hardware version of the virtual machine.
Upgrade to:	To upgrade, select a version from the drop-down menu.
Synchronize time	Select the check box to enable time synchronization between the virtual machine guest operating system and the virtual data center in which it is running.
Enter BIOS Setup	Select whether to force entry into the BIOS setup screen the next time the virtual machine boots. You can edit this property while the virtual machine is powered off.

5 Click **Save** once you complete making your changes.

Change the Hardware Properties of a Virtual Machine

You can review and change the hardware properties of a virtual machine.

Prerequisites

The virtual machine must be powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 In the card of the virtual machine you want to edit, click **Details**.

4 Click **Hardware** to expand the list of hardware properties that you can view and edit.

Option	Description
Number of virtual CPUs	Edit the number of CPUs. The maximum number of virtual CPUs that you can assign to a virtual machine depends on the number of logical CPUs on the host and the type of guest operating system that is installed on the virtual machine.
Cores per socket	Edit the cores per socket. You can configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on.

Option	Description
Expose hardware-assisted CPU virtualization to guest OS	You can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization.
Total Memory	Edit the memory resource settings for a virtual machine. The virtual machine memory size must be a multiple of 4 MB. This setting determines how much of the ESXi host memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size.
Memory hot add	If you enable memory hot-add, you can add memory resources to a virtual machine while the machine is powered on. This feature is only supported on certain guest operating systems and virtual machine hardware versions greater than 7.
Virtual CPU hot add	If you enable virtual CPU hot-add, you can add virtual CPUs to the virtual machine while it is powered on. You can add only multiples of the number of cores per socket. This feature is only supported on certain guest operating systems and virtual machine hardware versions.
Number of sockets	View the number of sockets. The number of sockets is determined by the number of virtual CPUs available. The number changes when you update the number of virtual CPUs.
Removable Media	View the available removable media, such as attached CD/DVD and floppy drive.

5 Under **Hard Disks**, click **Add** to add a hard disk and fill out the following details.

Option	Description
Size	Enter the hard disk size in MB.
Policy	The storage policy for the virtual machine is used. You can override this selection.
Bus Type	Select the bus type. The options are **Paravirtual (SCSI)**, **LSI Logic Parallel (SCSI)**, **LSI Logic SAS (SCSI)**, **IDE**, and **SATA**.
Bus Number	Enter the bus number.
Unit Number	Enter the logical unit number for the hard disk drive.

By default, all the hard disks attached to a virtual machine use the storage policy specified for the virtual machine. You can override this default for any of these disks when you create a virtual machine or modify its properties. The Size column for each hard disk includes a drop-down menu that lists all the storage policies available for this virtual machine.

6 Under **NICs**, click **Add**, and fill out the following details.

You can add up to 10 NICs. For information about the number of supported number of NICs depending on the virtual machine hardware version, see: http://kb.vmware.com/s/article/2051652. vCloud Director supports modifying virtual machine NICs while the virtual machine is running. For information about supported network adapter types, see http://kb.vmware.com/kb/1001805.

Option	Description
Primary NIC	A flag displays when the primary NIC is selected. Select a primary NIC. The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to virtual and physical machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.
NIC	Number of the NIC.
Connected	Select the check box to connect a NIC.
Network	Select a network from the drop-down menu.
IP Mode	Select an IP mode: ■ **Static - IP Pool** Pulls a static IP address from the network IP pool. ■ **Static - Manual** Allows you to specify a specific IP address manually. If you select this option, you must type an IP address in the **IP Address** column. ■ **DHCP** Pulls an IP address from a DHCP server.
MAC Address	Enter the network interface MAC address.

7 Click **Save**.

Change the Guest OS Customization Properties of a Virtual Machine

Guest OS customization on vCloud Director is optional for all platforms. It is required for virtual machines that must join a Windows domain.

Some of the information requested on this menu applies only to Windows platforms. The Guest OS Customization panel includes the information necessary for the virtual machine to join a Windows domain. An **organization administrator** can specify default values for a domain that Windows guests in that organization can join. Not all Windows virtual machines must join a domain, but in most enterprise installations, a virtual machine that is not a domain member cannot access many of the available network resources.

Prerequisites

- This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.
- Guest customization requires the virtual machine to be running VMware Tools.

- Before you can customize a Windows guest OS, your **system administrator** must install the appropriate Microsoft Sysprep files on the vCloud Director server group. See the *vCloud Director Installation and Upgrade Guide*.
- Customization of Linux guest operating systems requires that Perl is installed in the guest.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. In the card of the virtual machine you want to edit, click **Details**.
4. Click **Guest OS Customization and Properties** to expand the list of guest operating system settings.

Option	Description
Enable Guest Customization	You can select this option to enable guest customization.
Change SID	You can select this option to change the Windows Security ID (SID). This option is specific for virtual machines running a Windows guest operating system. The SID is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template on which it is based. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the machines are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.
Require Administrators to change password on first login	You can select this option to require administrators to change the password of the guest operating system on the first login. This is recommended for security purposes.
Allow local administrator password	You can select this option to allow setting an administrator password on the guest operating system. a Specify a password for the local administrator. Leaving the **Specify password** text box blank generates a password automatically. b Specify the number of times to allow automatic login. Entering a value of zero disables automatic login as an administrator.

Option	Description
Enable this VM to join a domain	You can select this option to join the virtual machine to a Windows domain. You can use the organization's domain or override the organization's domain and enter the domain properties. a Enter the domain name. b Enter the user name and password. c Enter the account organizational unit.
Script	You can use a customization script to modify the guest operating system of the virtual machine. When you add a customization script to a virtual machine, the script is called only on initial customization and force recustomization. If you set the precustomization command line parameter, the script is called before guest customization begins. If you set the postcustomization command line parameter, the script is called after guest customization finishes. ■ Click the upload button below the script text box to navigate to a customization script on your local machine. ■ Type the customization script directly into the **Script file** text box. A customization script that you enter directly into the **Script file** text box cannot contain more than 1500 characters. For more information, see VMware Knowledge Base article https://kb.vmware.com/kb/1026614.

5 Click **Save** once you complete making your changes.

Understanding Guest Customization

When you customize your guest operating system, there are some settings and options you should know about.

Enable Guest Customization Check Box

This check box is found on the **Guest OS customization** tab on the virtual machine **Properties** page. The goal of guest customization is to configure based on the options selected in the **Properties** page. If this check box is selected, guest customization and recustomization is performed when required.

This process is required for all guest customization features, such as the computer name, network settings, setting and expiring the administrator and root passwords, SID change for Windows Operating systems, and so on, to work. This option should be selected for **Power on and Force re-customization** to work.

If the check box is selected, and the virtual machine's configuration parameters in vCloud Director are out of sync with the settings in the guest OS, the **Profile** tab on the virtual machines **Properties** page displays that the settings out of sync with the guest OS and the virtual machine needs guest customization.

Guest Customization Behavior for vApps and Virtual Machines

The check boxes are deselected.

- **Enable guest customization**
- In Windows guest OSs, **Change SID**
- **Password reset**

If you want to perform a customization (or you made changes to network settings that need to be reflected in the guest OS), you can select the **Enable guest customization** check box and set the options on the **Guest OS Customization** tab of the virtual machine **Properties** page. When virtual machines from vApp templates are used to create a vApp and then add a virtual machine, the vApp templates act as building blocks. When you add virtual machines from the catalog to a new vApp, the virtual machines are enabled for guest customization by default. When you save a vApp template from a catalog as a vApp, virtual machines are enabled for guest customization only if the **Enable guest customization** check box is selected.

These are the default values of guest customization settings:

- The **Enable guest customization** check box is the same as the source virtual machine in your catalog.
- For Windows guest virtual machines, **Change SID** is the same as the source virtual machine in your catalog.
- The password reset setting is same as the source virtual machine in your catalog.

You can deselect the **Enable guest customization** check box if required before you start the vApp.

If blank virtual machines, which are pending guest OS installation, are added to a vApp, the **Enable guest customization** check box is deselected by default because these virtual machines are not yet ready for customization.

After you install the guest OS and VMware Tools, you can power off the virtual machines, stop vApp, and select the **Enable guest customization** check box and start the vApp and virtual machines to perform guest customization.

If the virtual machine name and network settings are updated on a virtual machine that has been customized, the next time you power on the virtual machine, it is recustomized, which resynchronizes the guest virtual machine with vCloud Director.

Power on and Force Recustomization of a Virtual Machine

You can power on a virtual machine and force the recustomization of a virtual machine.

If the settings in a virtual machine are not synchronized with vCloud Director or an attempt to perform a guest customization has failed, you can force the recustomization of the virtual machine.

Ensure that the application that is running in the virtual machine supports a recustomization. If you change a domain controller by using Microsoft Sysprep, and also change the SID, the virtual machine might be damaged. To mitigate the risk of damaging your virtual machine, create a snapshot before you recustomize it.

Prerequisites

- You must be an organization administrator.
- The virtual machine must be powered off.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **Power** menu of the virtual machine you want to power on and customize, select **Power On and Force Recustomization**.

The virtual machine is recustomized and powered on.

Change the Advanced Properties of a Virtual Machine

In the **Advanced** settings, you can configure the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine.

Use the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine.

Resource Allocation Shares	Shares specify the relative importance of a virtual machine within a virtual data center. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources. Shares are typically specified as High, Normal, or Low and these values specify share values with a 4:2:1 ratio, respectively. You can also select Custom to assign a specific number of shares (which expresses a proportional weight) to each virtual machine. When you assign shares to a virtual machine, you always specify the priority for that virtual machine relative to other powered-on virtual machines.
Resource Allocation Reservation	Specifies the guaranteed minimum allocation for a virtual machine. vCloud Director allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. The virtual data center guarantees that amount even when its resources are heavily loaded. The reservation is expressed in concrete units (megahertz or megabytes).

For example, assume that you have 2 GHz available and specify a resource allocation reservation of 1 GHz for virtual machine 1 and 1 GHz for virtual machine 2. Now each virtual machine is guaranteed to get 1 GHz if it needs it. However, if virtual machine 1 is using only 500 MHz, virtual machine 2 can use 1.5 GHz.

Reservation defaults to 0. You can specify a reservation if you need to guarantee that the minimum required amounts of CPU or memory are always available to the virtual machine.

Resource Allocation Limit

Specifies an upper bound for CPU and memory resources that can be allocated to a virtual machine. A virtual data center can allocate more than the reservation to a virtual machine, but never allocates more than the limit, even if there are unused resources on the system. The limit is expressed in concrete units (megahertz or megabytes).

CPU and memory resource limits default to unlimited. When the memory limit is unlimited, the amount of memory configured for the virtual machine when it was created becomes its effective limit in most cases.

In most cases, it is not necessary to specify a limit. You might waste idle resources if you specify a limit. The system does not allow a virtual machine to use more resources than the limit, even when the system is underutilized, and idle resources are available. Specify a limit only if you have good reasons for doing so.

Prerequisites

- A reservation pool virtual data center.
- Ensure that a certain amount of memory for a virtual machine is provided by the virtual data center.
- Guarantee that a particular virtual machine is always allocated a higher percentage of the virtual data center resources than other virtual machines.
- Set an upper bound on the resources that can be allocated to a virtual machine.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. In the card of the virtual machine you want to edit, click **Details**.
4. Click **Advanced**.

5 Set the resource allocations shares for the CPU settings.

Option	Description
Low	500 shares per virtual CPU.
Normal	1000 shares per virtual CPU.
High	2000 shares per virtual CPU.
Custom	Assign a specific number of shares by entering the number of shares (which expresses a proportional weight) to each virtual machine. When you assign shares to a virtual machine, you always specify the priority for that virtual machine relative to other powered-on virtual machines.

6 Specify the reservation for the CPU settings and, optionally, the limit for the CPU settings in MHz.

Option	Description
Unlimited	The default CPU resource option.
Maximum	Specify an upper bound for CPU resources that can be allocated to a virtual machine in MHz.

7 Set the resource allocations shares for the memory settings.

Option	Description
Low	5 shares per megabyte of configured virtual machine memory.
Normal	10 shares per megabyte of configured virtual machine memory.
High	20 shares per megabyte of configured virtual machine memory.
Custom	Assign a specific number of shares by entering the number of shares.

8 Specify the reservation for the memory settings and, optionally, the limit for the memory settings in MB.

Option	Description
Unlimited	The default CPU resource option.
Maximum	Specify an upper bound for CPU resources that can be allocated to a virtual machine in MHz.

9 Click **Add** under **Metadata** to specify the metadata, for example, you can add metadata about the creation date or owner.

10 Click **Save** once you complete making your changes.

Insert Media

You can insert media such as CD/DVD images from catalogs to use in a virtual machine guest operating system. You can use these media files to install an operating system in the virtual machine, various applications, drivers, and so on.

Prerequisites

You have access to a catalog with media files.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. Select the virtual machine where you want to add the media.
4. From the **More** menu, select **Insert Media**.
5. From the **Insert CD** window, select the media file to insert in the virtual machine.
6. Click **Insert**.

Eject Media

After you have finished using a CD or a DVD in your virtual machine, you can eject the media file.

Prerequisites

A media file was previously inserted to the virtual machine.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. Select the virtual machine from which you want to eject the media.
4. From the **More** menu, select **Eject Media**.

The media file is ejected.

Copy a Virtual Machine to a Different vApp

You can copy a virtual machine to another vApp. When you copy a virtual machine, the original virtual machine remains in the source vApp.

Prerequisites

- This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.
- Power off the VM.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **More** menu of the virtual machine you want to copy, select **Copy to**.
4. Select the destination vApp to which you want to copy the virtual machine, and click **Next**.
5. Configure the resources, such as name of the virtual machine and computer name, and, optionally, the storage policy and NICs, and click **Next**.

   Important The computer name can contain only alphanumeric characters and cannot consist of digits only.
6. On the Ready to Complete page review your settings and click **Done**.

Move a Virtual Machine to a Different vApp

You can move a virtual machine to another vApp. When you move a virtual machine, the original virtual machine is removed from the source vApp.

Starting with vCloud Director 9.5, moving VMs across different vApps relies on VMware vSphere® vMotion® and Enhanced vMotion Compatibility (EVC). You can move a VM to a different vApp that belongs to the same or another organization VDC within the same provider VDC.

While you are moving a virtual machine to a different vApp, you can perform reconfigurations such as changing the network and the storage profile.

Table 2-1. Reconfigurations During Virtual Machine Movements and Virtual Machine States

Reconfiguration	VM state if the target vApp is in the same organization VDC	VM state if the target vApp in another organization VDC within the same provider VDC
change the network	powered off	N/A
remove the network	powered on or off	N/A
change the storage profile	powered on or off	powered off

Prerequisites

- This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.
- Verify that the underlying vSphere resources support vMotion and EVC. For information about the requirements and limitations of vMotion and EVC, see *vCenter Server and Host Management*.

- If you want to change the VM network or the storage profile, check whether you must power off the VM. See table *Reconfigurations During VM Movements and VM States*.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **More** menu of the machine you want to move, select **Move to**.
4. Select the destination vApp and click **Next**.
5. Configure the resources, such as name of the virtual machine and computer name, and, optionally, the storage policy and NICs, and click **Next**.

   Important The computer name can contain only alphanumeric characters and cannot consist of digits only.

6. On the Ready to Complete page review your settings and click **Done**.

Virtual Machine Affinity and Anti-Affinity

Affinity and anti-affinity rules allow you to spread a group of virtual machines across different ESXi hosts or keep a group of virtual machines on a particular ESXi host.

An affinity rule places a group of virtual machines on a specific host so that you can easily audit the usage of those virtual machines. An anti-affinity rule places a group of virtual machines across different hosts, which prevents all virtual machines from failing at once in the event that a single host fails.

Affinity and anti-affinity rules are either required or preferred.

Required rule	If the affinity or anti-affinity rules cannot be satisfied, the virtual machines added to the rule do not power on.
Preferred rule	If the affinity or anti-affinity rules are violated, the cluster or host still powers on the virtual machines.

For example, if you have an anti-affinity rule between two virtual machines but only one physical host is available, a rule which is required (strong affinity) does not allow both virtual machines to power on. If the anti-affinity rule is preferred (weak affinity), both virtual machines are allowed to power on.

Related Videos

VM-VM Affinity in vCloud Director (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vcd_affinity_rules)

View Affinity and Anti-Affinity Rules

You can view existing affinity and anti-affinity rules and their properties, such as the virtual machines affected by the rules and whether the rules are enabled.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Affinity Rules** from the left panel.
2. (Optional) Click the **Grid editor** icon () and select what details about the rules you want to be displayed.

You see the list of the existing affinity and anti-affinity rules, whether they are required or not, virtual machines, and enabled status of each rule.

Create an Affinity Rule

Create an affinity rule to place a specific group of virtual machines on a single host so that you can audit the usage of those virtual machines.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Affinity Rules** from the left panel.
2. Under **Affinity Rules**, click **Create**.
3. Enter a name of the rule.
4. Deselect **Enabled** to create the rule without enabling it.

   By default, the check box is selected and rules are enabled after you create them.
5. Deselect **Required** to create a preferred rule, which means that the virtual machines added to the rule are powered on even when the rule is violated.

   By default, the check box is selected, and the rule is required. If the rule cannot be satisfied, the virtual machines added to the rule do not power on.
6. Select the virtual machines that you want to add to the affinity rule.
7. Click **Save**.

vCloud Director places the virtual machines associated with the affinity rule on a single host.

Create an Anti-Affinity Rule

Create an anti-affinity rule to place a specific group of virtual machines across multiple hosts to prevent simultaneous failure of those virtual machines in the event that a single host fails.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Affinity Rules** from the left panel.
2. Under **Anti-Affinity Rules**, click **Create**.
3. Enter a name of the rule.
4. Deselect **Enabled** to create the rule without enabling it.

   By default, the check box is selected and rules are enabled after you create them.
5. Deselect **Required** to create a preferred rule, and enable the cluster to power on the virtual machines even if the rule is violated.

   By default, the check box is selected, and the rule is required. If the rule cannot be satisfied, the virtual machines added to the rule do not power on.
6. Select the virtual machines to add to the anti-affinity rule.
7. Click **Save**.

vCloud Director places the virtual machines associated with the anti-affinity rule across multiple hosts.

Edit an Affinity or Anti-Affinity Rule

You can edit an affinity or anti-affinity rule to enable or disable the rule, add or remove virtual machines, change the rule name or the rule preference.

Prerequisites

This operation requires the Organization vDC: VM-VM Affinity Edit right. This right is included in the predefined **Catalog Author**, **vApp Author**, and **Organization Administrator** roles.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Affinity Rules** from the left panel.
2. Click the radio button next to the name of the rule that you want to edit and click **Edit**.
3. Edit the rule properties.
   a. Change the name of the rule as necessary.
   b. Select whether to enable or disable the rule.
   c. Select whether the rule should be required or preferred.
   d. Add more virtual machines or remove virtual machines.
4. Click **Save**.

Delete an Affinity or Anti-Affinity Rule

If you no longer want to use an affinity or anti affinity rule, you can delete it.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Affinity Rules** from the left panel.
2. Click the radio button next to the name of the rule that you want to delete and click **Delete**.
3. To confirm that you want to delete the rule, click **OK**.

vCloud Director deletes the affinity or anti-affinity rule.

Monitor Virtual Machines

If your vCloud Director administrator has enabled the feature for monitoring virtual machines, you can view the monitoring chart from the tenant portal.

Use this feature to understand the status of a given virtual machine over time (days, weeks, or months).

Prerequisites

This feature is only available if your vCloud Director administrator has enabled it.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.
2. Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. Select the virtual machine you want to monitor.
4. From the **More** menu, select **Details**.
5. Click the **Monitoring chart** menu to expand the view.

   The monitoring chart displays.
6. Below the chart, options for monitoring virtual machines display in a drop-down list. This list varies depending on the choices of your system administrator. You may see some or all of the following options.

Option	Description
Disk provisioned latest	Specified in KB. Choose from day, week, or month view.
Disk read average	Specified as a percentage. Choose from day, week, or month view.
Disk write average	Specified as a percentage. Choose from day, week, or month view.
CPU usage average	Specified as a percentage. Choose from day, week, or month view.

Option	Description
CPU usage MHZ average	Specified in MHZ. Choose from day, week, or month view.
CPU usage maximum	Specified as a percentage. Choose from day, week, or month view.
Mem usage average	Specified as a percentage. Choose from day, week, or month view.
Disk used latest	Specified in KB. Choose from day, week, or month view.

7 Select different options to display the values on the chart. You can also change the time frame displayed on the chart.

A new chart is displayed each time you select a different value from the list.

Working with Snapshots

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, the virtual machine is not affected and only an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines.

Snapshots are useful as a short-term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program.

You might want to use a snapshot when upgrading the operating system of a virtual machine. For example, before you upgrade the virtual machine, you take a snapshot to preserve the point in time before the upgrade. If there are no issues during the upgrade, you can choose to remove the snapshot, which will commit the changes you made during the upgrade. However, if you encountered an issue, you can revert to the snapshot, which will move back to your saved virtual machine state prior to the upgrade.

With vCloud Director you can have only one snapshot of a virtual machine. Each attempt to take a new snapshot of a virtual machine deletes the previous one.

Take a Snapshot of a Virtual Machine

You can take a snapshot of a virtual machine. After you take the snapshot, you can revert the virtual machine to the snapshot, or remove the snapshot.

Prerequisites

Verify that the virtual machine is not connected to an independent disk.

Note Snapshots do not capture NIC configurations.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine for which you want to take a snapshot, select **Create Snapshot**.

Taking a snapshot of a virtual machine replaces the existing snapshot if there is any.

4 Click **OK**.

The snapshot allows you to revert your virtual machine to the most recent snapshot.

Revert a Virtual Machine to a Snapshot

You can revert a virtual machine to the state it was in when the snapshot was created.

Prerequisites

The virtual machine has a snapshot.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine you want to revert to a snapshot, select **Revert to Snapshot**.

4 Click **OK**.

The virtual machine is reverted to the saved snapshot.

Remove a Snapshot of a Virtual Machine

You can remove a snapshot of a virtual machine.

When you remove a snapshot, you delete the state of the virtual machine that you preserved, and you can never return to that state again. Removing a snapshot does not affect the current state of the virtual machine.

Prerequisites

A virtual machine with a stored snapshot.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine for which you want to remove the snapshot, select **Remove Snapshot**.

4 Click **OK**.

Renew a Virtual Machine Lease

You can renew a virtual machine lease if the lease is expiring soon.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine with expiring lease, select **Renew Lease.**

The lease renews. You can see the new lease time frame in the **Lease** field.

Delete a Virtual Machine

You can delete a virtual machine from your organization.

Prerequisites

Your virtual machine must be powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and select **Virtual Machines** from the left panel.

2 Click  to view the list in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.

3 From the **More** menu of the virtual machine you want to delete, select **Delete**.

The virtual machine is deleted.

Working with vApps

A vApp consists of one or more virtual machines that communicate over a network and use resources and services in a deployed environment. A vApp can contain multiple virtual machines.

Starting with vCloud Director 9.5, vApps support IPv6 connectivity. You can assign IPv6 addresses to virtual machines connected to IPv6 networks.

Important All steps for working with vApps are documented from the card view, assuming that you have more than one virtual data center. Completing the same procedures from the grid view is also possible, but the steps might slightly vary.

This chapter includes the following topics:

- Delete a vApp

View vApps

You can view vApps in a grid view or in a card view.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. To view the vApps in a grid view, click  . To view them in a card view, click  .

   The list of vApps displays in a grid or as a list of cards.
3. (Optional) Configure the grid view to contain details you want to see.
   a. From the grid view, click the **Grid editor** icon ().
   b. Select the vApp details you want to include in the grid view by selecting the check box next to each detail you want to see.
   c. To save your changes, click **OK** .

   The selected details appear as columns for each vApp.
4. (Optional) From the grid view, click  on the left of a vApp, to display the actions you can take for the selected vApp.

   For example, you can shut down a vApp.

Build a New vApp

Instead of creating a vApp based on a vApp template, you can decide to create a new vApp using virtual machines from catalogs, new virtual machines, or a combination of both.

Building a vApp requires you to provide a name and optionally a description of the vApp. You can go back and add the virtual machines to the vApp at a later stage.

Prerequisites

This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click **Build New vApp**.

3 Enter a name and, optionally, a description for the vApp.

4 (Optional) Search the catalog for virtual machines to add to this vApp or add a new, blank virtual machine by clicking **Add Virtual Machine**.

   If there are no virtual machines in the catalog, create a virtual machine and add it to the vApp.

   a Enter the name and the computer name for the virtual machine.

   Important The computer name can contain only alphanumeric characters and cannot consist of digits only.

   b Select whether you want the virtual machine to power on right after it is created.

   c Enter a meaningful description.

   d Select how you want to deploy the virtual machine.

Option	Action
New	You deploy a new virtual machine with customizable settings. 1 Select an Operating System family and Operating System. 2 (Optional) Select a boot image. 3 Select the size of the virtual machine or click **Customize** to enter the compute, memory, and storage settings manually. The size of the virtual machine can be as small, medium, or large. 4 Specify the network settings for the virtual machine, such as network, IP mode, IP address, and primary NIC.
From Template	You deploy a virtual machine from a template that you select from the templates catalog.

   e To add the virtual machine to the vApp click **OK**.

   You can see the virtual machine added to the catalog.

5 (Optional) Repeat Step 4 for each additional virtual machine you want to create within the vApp.

6 To complete the creation of the vApp, click **Build**.

The vApp is created and is in a powered-off state. When you power on the vApp, the virtual machines in it are created and powered on as well.

Create a vApp From an OVF Package

You can create and deploy a vApp directly from an OVF package without creating a vApp template and a corresponding catalog item.

Prerequisites

Verify that you have an OVF package to upload and that you have permission to upload OVF packages and deploy vApps.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click **Add vApp from OVF**.
3. Click the **Upload** () button to browse to a location accessible from your computer, and select the OVF/OVA template file.

   The location might be your local hard drive, a network share, or a CD/DVD drive. The supported file extensions include .ova, .ovf, .vmdk, .mf, .cert, and .strings. If you select to upload an OVF file, which references more files than you are trying to upload, for example, a VMDK file, you must browse and select all files.
4. Click **Next**.
5. Verify the details of the OVF/OVA template you are about to deploy and click **Next**.
6. Enter a name and, optionally a description for the vApp, and click **Next**.
7. (Optional) Change the computer name of the vApp so that it contains only alphanumeric characters.

   This step is required only if the name of the vApp contains spaces or special characters. By default, the computer name is prepopulated with the name of the virtual machine. However, computer names must contain only alphanumeric characters.
8. From the **Storage Policy** drop-down menu, select a storage policy for each of the virtual machines in the vApp, and click **Next**.
9. Select the networks to which you want each virtual machine to connect. You can configure additional properties for virtual machines after you complete the wizard.

   You can optionally switch to the advanced networking workflow, and enter the network settings such as primary NIC, network adapter type, network, IP assignment and IP address manually.
10. Click **Next**.
11. Customize the hardware of the virtual machines in the vApp, and click **Next**.

Option	Description
Number of virtual CPUs	Enter the number of virtual CPUs for each virtual machine in the vApp. The maximum number of virtual CPUs that you can assign to a virtual machine depends on the number of logical CPUs on the host and the type of guest operating system that is installed on the virtual machine.
Cores per socket	Enter the number of cores per socket for each virtual machine in the vApp. You can configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on.

Option	Description
Number of cores	View the number of cores for each virtual machine in the vApp. The number changes when you update the number of virtual CPUs.
Total memory (MB)	Enter the memory in MB for each virtual machine in the vApp. This setting determines how much of the ESXi host memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size.

12 Review the settings on the Ready to Complete page, and click **Finish**.

The new vApp appears in the card view.

Create a vApp from a vApp Template

You can create a new vApp based on a vApp template stored in a catalog to which you have access.

If the vApp template is based on an OVF file that includes OVF properties for customizing its virtual machines, those properties are passed to the vApp. If any of those properties are user-configurable, you can specify the values.

Prerequisites

- Only organization administrators and vApp authors can access vApp templates in public catalogs.
- vApp users and above can access vApp templates in organization catalogs shared to them.

Procedure

1 From the main menu ☰), select **Libraries**, and select **vApp Templates** from the left panel.
The list of templates displays in a grid view.

2 Click the list bar (⋮) on the left of the vApp template you want to deploy as a vApp, and select **Create vApp**.

3 Enter a name and, optionally, a description of the vApp.

4 Select the virtual data center in which you want to create the vApp.

5 Select a storage policy.

6 Specify how long this vApp can run before it is automatically stopped.

7 Specify for how long the stopped vApp remains available before being automatically cleaned up.

8 Click **OK**.

Open a vApp

You can open a vApp to view the virtual machines and networks it contains. You can also view a diagram showing how the virtual machines and networks are connected.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the card view, you can see general information, such as the number of virtual machines associated with the vApp, lease information, total number of CPUs, total storage and memory, associated networks, and whether a snapshot is taken.
4. To view the detailed settings of a selected vApp, click **Details** on the vApp card.

Performing Power Operations on vApps

You can perform power operations on vApps, such as power on or off a vApp, suspending or resetting a vApp.

Power on a vApp

Powering on a vApp powers on all the virtual machines in the vApp that are not already powered on.

Prerequisites

You are at least a vApp author.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **Power** menu of the vApp you want to power on, select **Power On**.

The vApp is powered on.

Stop a vApp

Stopping a vApp powers off or shuts down all the virtual machines in the vApp. You must stop a vApp before you can perform certain actions. For example, adding the vApp to a catalog, copying it or moving it to another VDC.

Prerequisites

The vApp must be started.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **Power** menu of the vApp you want to stop, select **Power Off**.
4. Click **OK**.

All virtual machines in the vApp and the vApp itself are powered off.

Reset a vApp

Resetting a vApp clears state (memory, cache, and so on), but the vApp continues to run.

Prerequisites

Your vApp is started and virtual machines in it are powered on.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **Power** menu of vApp you want to reset, select **Reset**.

The state is cleared, and the vApp continues to run.

Suspend a vApp

Suspending a vApp preserves its current state by writing the memory to disk.

Prerequisites

The vApp is running.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.

3 From the **Power** menu of the vApp you want to suspend, select **Suspend**.

The vApp is suspended and its state is preserved.

Discard the Suspended State of a vApp

If a vApp is in a suspended state and you no longer have to resume the use of the vApp, you can discard the suspended state. Discarding the suspended state removes the saved memory and returns the vApp to a powered-off state.

Prerequisites

The vApp must be in a suspended state.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 From the **More** menu of the suspended vApp, select **Discard Suspended State**.

The state is discarded and the vApp is powered off.

Edit vApp Properties

You can edit the properties of an existing vApp, including the vApp name and description, lease settings, order in which to start the virtual machines in the vApp, sharing settings, and network settings.

Edit the General Properties of the vApp

You can review and change the name, description, and other general properties of a vApp.

Prerequisites

Verify that the vApp is powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected vApp, click **Details** to view and edit the vApp properties.

4 Review and change the properties as needed, and click **Save**.

Option	Action
Name	Enter a new name for the vApp.
Description	Type an optional description of the vApp.
Snapshot	If there is a snapshot, details for it display.
Leases	Select **Renew** to renew the lease. a Schedule the runtime lease in number of days. Defines how long the vApp can run before it is automatically stopped b Schedule the storage lease in number of days. Defines the number of days in which the vApp remains available before being automatically deleted.

The general settings are saved.

Edit vApp Advanced Properties

You can configure the start and stop order of virtual machines within your vApp. Configure the start and stop order in case you have applications installed in the virtual machines that must start and stop in a particular order.

These settings are useful if you need to start and stop your virtual machines in a particular order. For example, one virtual machine houses a database server, another houses an application server, and the last houses a web server. In order for the related functions to work properly, the database server must start first, the application server must start second, and the web server must start last.

Prerequisites

Verify that the vApp is powered off.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected vApp, click **Details** and scroll down to the vApp advanced properties.

4 Enter the start and stop order properties for each virtual machine, and click **Save**.

Option	Action
Start Order	Enter the order in which you want the virtual machine to start. You must enter a value for each machine in the sequence.
Start Action	Enter the start action you want to use when starting the machine. The start action is the action the virtual machine takes upon starting.

Option	Action
Start Wait	Enter the start wait time. The start wait time is the amount of time you want to wait before you start the next machine in the sequence.
Stop Action	Enter the stop action. The stop action is the action the virtual machine takes upon stopping. If you select **Power Off**, the machine powers off without performing shutdown actions that ensure stability (which is the equivalent of pulling a plug out of a socket). Select this action if you have not installed VMware Tools. Otherwise, select **Shut Down**, which ensures stability upon shutting down.
Stop Wait	Enter the stop wait time. The stop wait time is the amount of time to wait before you shut down the next virtual machine in the sequence.

Share a vApp

You can share your vApps with other groups or users within your organization. The access controls that you set, determine the operations that can be completed on the shared vApps.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected vApp, click **Details**, and scroll down to the sharing properties of the vApp.
4. Select the users with whom you want to share the vApp and click **Save**.

Option	Action
Share with everyone in the organization	Select this option to share with all users in the organization.
Share with specific users and groups	Select this option to share only with users that you specify. a Select the names from the **Users and groups with no access** panel to move them to the **Users and groups with access** panel. b Select an access level for the specified users and groups. ■ To grant full control, select **Full Control**. Users with full control can open, start, save a vApp as a vApp template, add the template to a catalog, change the owner of the vApp, copy to a catalog, and modify properties. ■ To grant read-only access, select **Read Only**.

Your vApp is shared with the specified users or groups.

Work with Snapshots

Creating a snapshot preserves the state and data of the virtual machines within a vApp at a specific point in time. A snapshot is not intended to be used for long periods of time or in place of backing up the vApp.

You might want to use a snapshot when upgrading the virtual machines in a vApp. For example, before you upgrade the virtual machines, you create a snapshot to preserve the point in time before the upgrade. To do this, you save a snapshot prior to upgrading, and then perform the upgrade. If there are no issues during the upgrade, you can choose to remove the snapshot, which will commit the changes you made during the upgrade. However, if you encountered an issue, you can revert the snapshot, which will move back to your saved vApp state prior to the upgrade.

Take a Snapshot of a vApp

By taking a snapshot of a vApp, you take snapshots of all virtual machines in the vApp. After you take the snapshot, you can revert all virtual machines in the vApp to the snapshot, or remove the snapshot if you do not need it.

vApp snapshots have some limitations.

- vApp snapshots do not capture NIC configurations.
- If any virtual machine in the vApp is connected to an independent disk, you cannot take a vApp snapshot.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp for which you want to take a snapshot, select **Create Snapshot**.

   Taking a snapshot of a vApp replaces the existing snapshot, if there is any.
4. Click **OK**.

A snapshot of the vApp is created.

What to do next

You can revert all the virtual machines in the vApp to the most recent snapshot.

Revert a vApp to a Snapshot

You can revert all virtual machines in a vApp to the state they were in when you created the vApp snapshot.

Prerequisites

Verify that the vApp has an existing snapshot.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp you want to revert, select **Revert to Snapshot**.
4. Click **OK.**

All virtual machines in the vApp are reverted to the snapshot state.

Remove a Snapshot of a vApp

You can remove a snapshot of a vApp.

When you remove a vApp snapshot, you delete the state of the virtual machines in the vApp snapshot and you can never return to that state again. Removing a snapshot does not affect the current state of the vApp.

Prerequisites

You have taken a snapshot of the vApp.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp for which you want to remove a snapshot, select **Remove Snapshot**.

The snapshot is removed.

Change the Owner of a vApp

You can change the owner of the vApp, for example, when a vApp owner leaves the company or changes roles within the company.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp for which you want to change the owner, select **Change owner**.
4. Select a user from the list.
5. Click **OK**.

The owner of the vApp is changed.

Move a vApp to Another Virtual Data Center

When you move a vApp to another virtual data center, the vApp is removed from the source virtual data center.

Prerequisites

- You are at least a **vApp author**.
- Your vApp is powered off.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp you want to move, select **Move to**.
4. Select the virtual data center where you want to move the vApp.
5. Click **OK**.

The vApp is removed from the source data center and moved to the target data center.

Copy a Stopped vApp to Another Virtual Data Center

When you copy a vApp to another virtual data center, the original vApp remains in the source virtual data center.

Prerequisites

- You are at least a **vApp author**.
- The vApp is powered off.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp you want to copy, select **Copy to**.
4. Type a name and description.
5. Select the virtual data center in which you want to create the copy of the vApp.
6. Click **OK**.

The vApp is copied with the name and description you provided to the specified virtual data center.

Copy a Powered-On vApp

To create a vApp based on an existing vApp, you can copy a vApp and change the copy so that the copy meets your needs. You do not have to power off virtual machines in the vApp before you copy the vApp. The memory state of running virtual machines is preserved in the copied vApp.

Prerequisites

Verify that the following conditions are met.

- You are at least a **vApp user**.
- The organization virtual data center is backed up by vCenter Server 5.5 or later.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp you want to copy, select **Copy to**.
4. Type a name and description.
5. Select a virtual data center in which you want to create the copy of the vApp.
6. Select a storage policy.
7. Click **OK**.

A copy of the vApp is created and the vApp copy is in a suspended state. The copied vApp is enabled for network fencing.

What to do next

Modify the network properties of the new vApp or power on the vApp.

Add a Virtual Machine to a vApp

You can add a virtual machine to a vApp.

Prerequisites

You must be an **organization administrator** or **vApp author** to access virtual machines in public catalogs.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp to which you want to add a virtual machine, select **Add VM**.

   The list of virtual machines that are associated to the vApp displays in the **Add VMs** window.
4. To create a new virtual machine and associate it with the vApp automatically, click **Add Virtual Machine**.
5. Enter the name and the computer name for the virtual machine.

   Important The computer name can contain only alphanumeric characters and cannot consist of digits only.
6. Select whether you want the virtual machine to power on right after it is created.
7. (Optional) Enter a meaningful description.
8. Select how you want to deploy the virtual machine.

Option	Action
New	You deploy a new virtual machine with customizable settings. a Select an Operating System family and Operating System. b (Optional) Select a Boot image. c Select the size of the virtual machine or click **Customize** to enter the compute, memory, and storage settings manually. The size of the virtual machine can be as small, medium, or large. d Specify the network settings for the virtual machine, such as network, IP mode, IP address, and primary NIC. You can keep the default network configuration that uses the Org VDC network assigned to the vApp.
From Template	You deploy a virtual machine from a template that you select from the templates catalog.

9. Click **OK** to create the virtual machine.

Save a vApp as a vApp Template to a Catalog

By adding a vApp to a catalog, you convert the particular vApp to a vApp template.

Prerequisites

- This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.
- Your organization must have a catalog and a virtual data center with available space.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp you want to add to a catalog, select **Add to Catalog**.

   Note You can add vApps to a catalog even if the virtual machines that belong to the vApp are in a running state. However, if you select a running vApp, it is added to the catalog as a vApp template and all the virtual machines are in a suspended state.
4. Select the destination catalog from the **Catalog** drop-down menu.
5. Enter a name and, optionally, a description for the vApp template.
6. (Optional) Select **Overwrite catalog item** if you want the new catalog item to overwrite any existing vApp template and select the catalog item to overwrite.

   For example, when you upload a new version of a vApp to the catalog you might want to overwrite the old version.
7. Specify how the template will be used.

   The setting applies when you are creating a vApp based on the vApp template. It is ignored when you build a vApp by using individual virtual machines from this template.

Option	Description
Make identical copy	Select to make an identical copy of the vApp when you create a vApp from the vApp template.
Customize VM settings	Select to enable customization of the virtual machine settings when you create a vApp from the vApp template.

8. Click **OK** to complete the creation of the vApp template.

The vApp is saved as a vApp template and appears in the specified catalog.

Download a vApp as an OVF Package

You can download a vApp as an OVF package.

Prerequisites

- This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.
- Verify that the vApp is powered off and undeployed.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. From the **More** menu of the vApp that you want to download, select **Download**.
4. (Optional) Select **Preserve identity information** to include the UUIDs and MAC addresses of the vApp's virtual machines in the downloaded OVF package.
5. Click **OK** to confirm the selection and finish the download.

Working with Networks in a vApp

The virtual machines in a vApp can connect to vApp networks (isolated or routed) and organization virtual data center networks (direct or fenced). You can add networks of different types to a vApp to address multiple networking scenarios.

Virtual machines in the vApp can connect to the networks that are available in a vApp. If you want to connect a virtual machine to a different network, you must first add it to the vApp.

A vApp can include vApp networks and organization virtual data center networks. A vApp network can be isolated or routed. An isolated vApp network is contained within the vApp. You can also route a vApp network to an organization virtual data center network to provide connectivity to virtual machines outside of the vApp. For routed vApp networks, you can configure network services, such as a firewall and static routing.

You can connect a vApp directly to an organization virtual data center network. If you have multiple vApps that contain identical virtual machines connected to the same organization virtual data center network and you want to start the vApps at the same time, you can fence the vApp. Fencing the vApp allows you to power on the virtual machines without conflict, by isolating their MAC and IP addresses.

View vApp Networks

You can access and view the networks in a vApp.

Prerequisites

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected vApp, click **Details**.
4. Click the **Networks** tab.

   The list of networks, if there are any, is displayed. You can view information about each network, such as name, gateway, netmask, connection and retain IP and NAT resources.
5. (Optional) To edit the columns to see, click the **Grid editor** icon () and select or deselect the check boxes of the columns you want to be displayed or hidden, respectively.

Add Network to a vApp

You can add a network to a vApp to make the network available to the virtual machines in the vApp. You can add a vApp network or an organization virtual data center network to a vApp.

Connections can be direct or fenced. Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.

When fencing is enabled and the vApp is powered on, an isolated network is created from the organization virtual data center network pool. This allows a router to pass traffic between two networks by using the same IP space.

Prerequisites

To add an organization virtual data center network, your administrator must have created such a network.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected vApp, click **More** and select **Add network**.

4 Select the type of network to add.

Option	Action
Organization VDC Network	Select an organization virtual data center network from the list.
vApp Network	a Enter a name and, optionally, a description for the network. b Enter the gateway and network mask. c (Optional) Enter the primary and secondary DNS, and the DNS suffix. d (Optional) Select whether to allow guest VLAN. e (Optional) Enter static IP pool settings, such as IP ranges.

5 Click **Add**.

The network is added to the vApp.

What to do next

Connect a virtual machine in the vApp to the network.

Configuring Network Services for a vApp Network

You can configure network services, such as DHCP, firewalls, network address translation (NAT), and static routing for certain vApp networks.

The network services available depend on the type of vApp network.

Table 3-1. Network Services Available by Network Type

vApp Network Type	DHCP	Firewall	NAT	Static Routing
Direct				
Routed	X	X	X	X
Isolated	X			

View and Edit General Network Details

You can view and edit the general vApp network details, for example the network name and description.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected virtual appliance, click **Details**.

4 On the **Networks** tab, click a network to view the network details.

5 On the **General** tab, review the network information.

6 Click **Edit**.

7 Edit the vApp network name and description.

8 Click **Save**.

Edit the Static IP Pool Settings of a vApp Network

You can configure a vApp network to provide static IP addresses to the virtual machines in the vApp by pulling them from a static pool of IP addresses.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected virtual appliance, click **Details**.

4 On the **Networks** tab, click a network to view the network details.

5 On the **IP Management** tab, click **Static Pools**.

6 Click **Edit**.

7 Enter an IP range and click **Add**.

8 Click **Save**.

Edit the DNS Settings of a vApp Network

After you create e vApp network, you can view and edit the DNS settings at any time.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected virtual appliance, click **Details**.

4 On the **Networks** tab, click a network to view the network details.

5 On the **IP Management** tab, click **DNS**.

The DNS settings are displayed.

6 Click **Edit**.

7 Edit the primary and secondary DNS, and the DNS suffix.

8 Click **Save**.

Configure DHCP for a vApp Network

You can configure certain vApp networks to provide DHCP services to virtual machines in the vApp.

When you enable DHCP for a vApp network, connect a NIC on virtual machine in the vApp to that network, and select DHCP as the IP mode for that NIC. vCloud Director assigns a DHCP IP address to the virtual machine when you power it on.

Prerequisites

A routed vApp network or an isolated vApp network.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected virtual appliance, click **Details**.
4. On the **Networks** tab, click a network to view the network details.
5. On the **IP Management** tab, click **DHCP**.

   The DHCP status is displayed.
6. Click **Edit**.
7. Click **Enabled**.
8. In the **IP Pool** text box, enter a range of IP addresses.

   vCloud Director uses these addresses to satisfy DHCP requests. The range of DHCP IP addresses cannot overlap with the static IP pool for the vApp network.
9. Set the default and maximum lease time in seconds.
10. Click **Save**.

Display the IP Allocations for Your vApp Network

You can review the IP allocations for the networks in your vApp.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected virtual appliance, click **Details**.
4. On the **Networks** tab, click a network to view the network details.

5 On the **IP Management** tab, click **IP Allocations**.

The allocated IP addresses are displayed.

Configure Static Routing for a vApp Network

You can configure certain vApp networks to provide static routing services to allow virtual machines on different vApp networks to communicate.

Any static route that you create is automatically enabled.

Prerequisites

A routed vApp network.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected virtual appliance, click **Details**.

4 On the **Networks** tab, click a network to view the network details.

5 On the **Routing** tab, click **Edit**.

You can enable or disable static routing for the network.

Add Static Routing for a vApp Network

You can add static routes between two vApp networks that are routed to the same organization virtual data center network. Static routes allow traffic between the networks.

You cannot add static routes to a fenced vApp or between overlapping networks. After you add a static route to a vApp network, configure the network firewall rules to allow traffic on the static route. For vApps with static routes, select to use assigned IP addresses until the vApp or associated networks are deleted.

Static routes function only when the vApps containing the routes are running. If you change the parent network of a vApp, delete a vApp, or delete a vApp network, and the vApp includes static routes, those routes cannot function and you must remove them manually.

Prerequisites

- Two vApp networks are routed to the same organization virtual data center network.
- The vApp networks are in vApps that were started at least once.
- Static routing is enabled on both vApp networks.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.

2 Click  to view the vApps in a card view.

3 In the card of the selected virtual appliance, click **Details**.

4 On the **Networks** tab, click a network to view the network details.

5 On the **Routing** tab, under Static Routing click **Add**.

The allocated IP addresses are displayed.

6 Enter a name of the static route.

7 Enter the network address in CIDR format.

The network address is for the vApp network to which to add a static route.

8 Enter the next hop IP address.

The next hop IP address is the external IP address of that vApp network's router.

9 Click **Save**.

10 Repeat the same procedure for the second vApp network.

Example: Static Routing Example

vApp Network 1 and vApp Network 2 are both routed to Org Network Shared. You can create a static route on each vApp network to allow traffic between the networks. You can use information about the vApp networks to create the static routes.

Table 3-2. Network Information

Network Name	Network Specification	Router External IP Address
vApp Network 1	192.168.1.0/24	192.168.0.100
vApp Network 2	192.168.2.0/24	192.168.0.101
Org Network Shared	192.168.0.0/24	NA

On vApp Network 1, create a static route to vApp Network 2. On vApp Network 2, create a static route to vApp Network 1.

Table 3-3. Static Routing Settings

vApp Network	Route Name	Network	Next Hop IP Address
vApp Network 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp Network 2	tovapp1	192.168.1.0/24	192.168.0.100

Delete a vApp Network

If you no longer need a network in your vApp, you can delete the network.

Prerequisites

The vApp is stopped and no virtual machines in the vApp are connected to the network.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Click  to view the vApps in a card view.
3. In the card of the selected virtual appliance, click **Details**.
4. Select the network that you want to delete, click **Delete**, and confirm the deletion.

Renew a vApp Lease

You can renew a vApp lease if the lease has expired.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Select the vApp you want to renew.
3. From the **More** menu, select **Renew Lease.**

The lease renews. You can see the new lease timeframe in the **Lease** field.

Delete a vApp

You can delete a vApp, which removes it from your organization.

Prerequisites

Your vApp must be stopped.

You must be at least a **vApp author**.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **vApps** from the left panel.
2. Select the vApp you want to delete.
3. From the **More** menu, select **Delete**.
4. Click **OK**.

The vApp is deleted.

Managing Organization VDC Networks

Organization virtual data center networks are created and assigned to your organization virtual data center by a **system administrator** or an **organization administrator**. An **organization administrator** can view information about networks, configure network services, and more.

You can use direct, routed, internal, or cross-VDC organization virtual data center networks.

Table 4-1. Types of Organization Virtual Data Center Networks

Data Center Type Network	Description
Direct	Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network. This network provides direct layer 2 connectivity to virtual machines outside of the organization. Virtual machines outside of this organization can connect to virtual machines in the organization directly. **Note** Only your service provider can add a direct organization VDC network. You cannot add this type of organization VDC network from the Tenant Portal. Can be IPv4 or IPv6.
Isolated (Internal)	Accessible only by the same organization. Only virtual machines in this organization can connect to and see traffic on the internal network. The internal network provides an organization with an isolated, private network that multiple virtual machines and vApps can connect to. This network provides no connectivity to virtual machines outside the organization. Machines outside of the organization have no connectivity to machines in the organization. Can be IPv4 only.

Table 4-1. Types of Organization Virtual Data Center Networks (Continued)

Data Center Type Network	Description
Routed	Accessible only by the same organization. Only virtual machines in this organization can connect to this network. This network also provides controlled access to an external network. System administrators and organization administrators can configure network address translation (NAT), firewall, and VPN settings to make specific virtual machines accessible from the external network. Can be IPv4 or IPv6.
Cross-VDC	This network is part of a stretched network spanning a data center group. A data center group can comprise between two and four organization virtual data centers in a single or multisite vCloud Director deployment. Virtual machines connected to this network are connected to the underlying stretched network. Can be IPv4 only.

All steps for managing your organization virtual data center networks are documented assuming that you have more than one virtual data center.

This chapter includes the following topics:

Add an Isolated Organization Virtual Data Center Network

You can add an isolated organization VDC network, which is accessible only by this organization. This network provides no connectivity to virtual machines outside this organization. Virtual machines outside of this organization have no connectivity to the virtual machines in the organization.

You can add a mix of isolated and routed organization VDC networks to meet the needs of your organization.

You can create an isolated VDC network that is backed by a network pool.

You can create only an IPv4 isolated organization VDC network.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Networks** from the left panel.

2 Click **New**.

3 Enter the Organization VDC network settings.

Option	Action
Org VDC	Select an organization virtual data center from the drop-down menu.
Name	Enter a meaningful name for your organization VDC network.
Description	Optionally, enter a description for the organization VDC network.
Share this network with other VDCs in this organization	Select this option if you want to make the organization VDC network available to other virtual data centers in the organization. One potential use case for this option is when an application exists within an Organization VDC that has a reservation or allocation pool set as the allocation model. In this case, it might not have enough room to run more virtual machines. As a solution, you can create a secondary Organization VDC with pay-as-you-go and run more virtual machines on that network on a temporary basis. **Note** The Organization VDCs must be backed by the same Provider VDC.
Type	Select **Isolated network within this virtual data center**.

4 Enter the network gateway Classless Inter-Domain Routing (CIDR) settings.

Use the format *network_gateway_IP_address*/*subnet_prefix_length*, for example, **192.167.1.1/24**.

This option is available only if the gateway has the Use default gateway for DNS relay property enabled.

5 (Optional) Configure the DNS settings.

Option	Action
Primary DNS	Enter the IP address for your primary DNS server.
Secondary DNS	Enter the IP address for your secondary DNS server.
DNS Suffix	Enter your DNS suffix. The DNS suffix is the DNS name without including the hostname.

6 (Optional) To reserve one or more IP addresses for assignment to virtual machines that require static IP addresses, configure the **Static IP Pool** for this network.

a Enter the address or range of addresses, and click **Add**.

b To add multiple static IP addresses or ranges, repeat this step.

Secure Access Using Virtual Private Networks

In a vCloud Director environment, you can create VPN tunnels between:

- Organization virtual data center networks on the same organization
- Organization virtual data center networks on different organizations
- Between an organization virtual data center network and an external network

---

1 Add an SSL VPN-Plus Client Installation Package

Use the Installation Packages screen on the **SSL VPN-Plus** tab in the vCloud Director tenant portal to create named installation packages of the SSL VPN-Plus client for the remote users.

2 Edit SSL VPN-Plus Client Configuration

Use the **Client Configuration** screen on the **SSL VPN-Plus** tab in the vCloud Director tenant portal to customize the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

How to Use Client Certificates

You can create a client certificate through a CAI command or REST call. You can then distribute this certificate to your remote users, who can install the certificate on their web browser.

The main benefit of implementing client certificates is that a reference client certificate for each remote user can be stored and checked against the client certificate presented by the remote user. To prevent future connections from a certain user, you can delete the reference certificate from the security server list of client certificates. Deleting the certificate denies connections from that user.

Working with Security Tags

Security tags are labels which can be associated with a virtual machine or a group of virtual machines. Security tags are designed to be used with security groups. Once you create the security tags, you associate them with a security group which can be used in firewall rules. You can create, edit, or assign a user-defined security tag. You can also view which virtual machines or security groups have a particular security tag applied.

A common use case for security tags is to dynamically group objects to simplify firewall rules. For example, you might create several different security tags based on the type of activity you expect to occur on a given virtual machine. You create a security tag for database servers and another one for email servers. Then you apply the appropriate tag to virtual machines that house database servers or email servers. Later, you can assign the tag to a security group, and write a firewall rule against it, applying different security settings depending on whether the virtual machine is running a database server or an email server. Later, if you change the functionality of the virtual machine, you can remove the virtual machine from the security tag rather than editing the firewall rule.

Create and Assign Security Tags

You can create a security tag and assign it to a virtual machine or a group of virtual machines.

You create a security tag and assign it to a virtual machine or a group of virtual machines.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and under **Networking**, select **Security**.
2. Select a security service, and click **Configure services**.
3. Click the **Security Tags** tab.
4. Click the **Create** () button, and enter a name for the security tag.
5. (Optional) Enter a description for the security tag.
6. (Optional) Assign the security tag to a virtual machine or a group of virtual machines.

   In the **Browse objects of type** drop-down menu, **Virtual Machines** is selected by default.

   a. Select a virtual machine from the left panel.

   b. Assign the security tag to the selected virtual machine by clicking the right arrow.

      The virtual machine moves to the right panel and is assigned the security tag.
7. When you complete assigning the tag to the selected virtual machines, click **Keep**.

The security tag is created, and if you chose, is assigned to selected virtual machines.

What to do next

Security tags are designed to work with a security group. For more information about creating security groups, see Create a Security Group.

Change the Security Tag Assignment

After you create a security tag, you can manually assign it to virtual machines. You can also edit a security tag to remove the tag from the virtual machines to which you have already assigned it.

If you have created security tags, you can assign them to virtual machines. You can use security tags to group virtual machines for writing firewall rules. For example, you might assign a security tag to a group of virtual machines with highly sensitive data.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and under **Networking**, select **Security**.
2. Select a security service, and click **Configure services**.

3 Click the **Security Tags** tab.

4 From the list of security tags, select the security tag that you want to edit, and click the **Edit** () button..

5 Select virtual machines from the left panel, and assign the security tag to them by clicking the right arrow.

   The virtual machines in the right panel are assigned the security tag.

6 Select virtual machines in the right panel, and remove the tag from them by clicking the left arrow.

   The virtual machines in the left panel do not have the security tag assigned.

7 When you finish adding your changes, click **Keep**.

The security tag is assigned to the selected virtual machines.

What to do next

Security tags are designed to work with a security group. For more information about creating security groups, see Create a Security Group.

View Applied Security Tags

You can view the security tags applied to virtual machines in your environment. You can also see the security tags that are applied to security groups in your environment.

Prerequisites

A security tag must have been created and applied to a virtual machine or to a security group.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and under **Networking**, select **Security**.

2 Select a security service, and click **Configure services**.

3 View the assigned tags from the **Security Tags** tab.

   a On the **Security Tags** tab, select the security tag for which you want to see assignments, and click the **Edit** icon.

   b Under the **Assign/Unassign VMs**, you can see the list of virtual machines assigned to the security tag.

   c Click **Discard**.

4 View the assigned tags from the **Security Groups** tab.

   a Click the **Grouping Objects** tab, and click **Security Groups**.

   b Select a security group.

   c From the list under **Include Members**, you can see the security tag assigned to a security group.

You can view the existing security tags and associated virtual machines and security groups. This way, you can determine a strategy for creating firewall rules based on security tags and security groups.

Edit a Security Tag

You can edit a user-defined security tag.

If you change the environment or function of a virtual machine, you might also want to use a different security tag so that firewall rules are correct for the new machine configuration. For example, if you have a virtual machine where you no longer store sensitive data, you might want to assign a different security tag so that firewall rules that apply to sensitive data is no longer run against the virtual machine.

Procedure

1 On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and under **Networking**, select **Security**.

2 Select a security service, and click **Configure services**.

3 Click the **Security Tags** tab.

4 From the list of security tags, select the security tag that you want to edit.

5 Click the **Edit** () button.

6 Edit the name and the description of the security tag.

7 Assign the tag to or remove the assignment from the virtual machines that you select.

8 To save your changes, click **Keep**.

What to do next

If you edit a security tag, you might also need to edit an associated security group or firewall rules. For more information about security groups, see Working with Security Groups

.

Delete a Security Tag

You can delete a user-defined security tag.

You might want to delete a security tag if the function or environment of the virtual machine changes. For example, if you have a security tag for Oracle databases, but you decide to use a different database server, you can remove the security tag so that firewall rules that apply to Oracle databases no longer run against the virtual machine.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and under **Networking**, select **Security**.
2. Select a security service, and click **Configure services**.
3. Click the **Security Tags** tab.
4. From the list of security tags, select the security tag that you want to delete.
5. Click the **Delete** () button.
6. To confirm the deletion, click **OK**.

The security tag is deleted.

What to do next

If you delete a security tag, you might also need to edit an associated security group or firewall rules. For more information about security groups, see Working with Security Groups.

Working with Security Groups

A security group is a collection of assets or grouping objects, such as virtual machines, organization virtual data center networks, or security tags.

Security groups can have dynamic membership criteria based on security tags, virtual machine name, virtual machine guest OS name, or virtual machine guest host name. For example, all virtual machines that have the security tag "web" will be automatically added to a specific security group destined for Web servers. After creating a security group, a security policy is applied to that group.

Create a Security Group

You can create user-defined security groups.

Prerequisites

If you want to use security tags with security groups, the tags should be created before creating the security group. For information about creating security tags, see Change the Security Tag Assignment.

Procedure

1 Open the Security Services.

   a Navigate to **Networking > Security**.

   b Select the organization VDC for which you want to apply security settings, and click **Configure Services**.

      The tenant portal opens Security Services.

2 Navigate to **Grouping Objects > Security Groups**

   The **Security Groups** page opens.

3 Click the **Create** () button.

4 Enter a name and, optionally, a description for the security group.

   The description displays in the list of security groups, so adding a meaningful description can make it easy to identify the security group at a glance.

5 (Optional) Add a dynamic member set.

   a Click the **Add** () button under Dynamic Member Sets.

   b Select whether to match **Any** or **All** of the criteria in your statement.

   c Enter the first object to match.

      The options are **Security Tag**, **VM Guest OS Name**, **VM Name**, and **VM Guest Host Name**.

   d Select an operator, such as **Contains**, **Starts with**, or **Ends with**.

   e Enter a value.

   f (Optional) To add another statement, use a Boolean operator **And** or **Or**.

6 (Optional) Include Members.

   a From the **Browse objects of type** drop-down menu, select the type of objects, such as **Virtual Machines**, **Org VDC networks**, **IP sets**, **MAC sets**, or **Security tags**.

   b To include an object in the Include Members list, select the object from the left panel, and move it to the right panel by clicking the right arrow.

7 (Optional) Exclude members.

   a From the **Browse objects of type** drop-down menu, select the type of objects, such as **Virtual Machines**, **Org VDC networks**, **IP sets**, **MAC sets**, or **Security tags**.

   b To include an object in the Exclude Members list, select the object from the left panel, and move it to the right panel by clicking the right arrow.

8 Click **Keep** to preserve your changes.

   The operation can take a minute to complete.

The security group can now be used in rules, such as firewall rules.

Edit a Security Group

You can edit user-defined security groups.

Prerequisites

You must have created user-defined security groups.

Procedure

1 Open the Security Services.

   a Navigate to **Networking > Security**.

   b Select the organization VDC for which you want to apply security settings, and click **Configure Services**.

   The tenant portal opens Security Services.

2 Navigate to **Grouping Objects > Security Groups**

   The **Security Groups** page opens.

3 Select the security group you want to edit.

   The details for the security group display below the list of security groups.

4 (Optional) Edit the name and the description of the security group.

5 (Optional) Add a dynamic member set.

   a Click the **Add** () button under **Dynamic Member Sets**.

   b Select whether to match **Any** or **All** of the criteria in your statement.

   c Enter the first object to match.

   The options are **Security Tag**, **VM Guest OS Name**, **VM Name**, and **VM Guest Host Name**.

   d Select an operator, such as **Contains**, **Starts with**, or **Ends with**.

   e Enter a value.

   f (Optional) To add another statement, use a Boolean operator **And** or **Or**.

6 (Optional) Edit a dynamic member set by clicking the **Edit**) icon next to the member set that you want to edit.

   a Apply the necessary changes to the dynamic member set.

   b Click **OK**.

7 (Optional) Delete a dynamic member set by clicking the **Delete**) icon next to the member set that you want to delete.

8 (Optional) Edit the included members list by clicking the **Edit**) icon next to the Include Members list.

   a From the **Browse objects of type** drop-down menu, select the type of objects, such as **Virtual Machines**, **Org VDC networks**, **IP sets**, **MAC sets**, or **Security tags**.

   b To include an object in the include members list, select the object from the left panel, and move it to the right panel by clicking the right arrow.

   c To exclude an object from the include members list, select the object from the right panel, and move it to the left panel by clicking the left arrow.

9 (Optional) Edit the excluded members list by clicking the **Edit**) icon next to the Exclude Members list.

   a From the **Browse objects of type** drop-down menu, select the type of objects, such as **Virtual Machines**, **Org VDC networks**, **IP sets**, **MAC sets**, or **Security tags**.

   b To include an object in the exclude members list, select the object from the left panel, and move it to the right panel by clicking the right arrow.

   c To exclude an object from the exclude members list, select the object from the right panel, and move it to the left panel by clicking the left arrow.

10 Click **Save changes**.

   The changes to the security group are saved.

Delete a Security Group

You can delete a user-defined security group.

Procedure

1 Open the Security Services.

   a Navigate to **Networking > Security**.

   b Select the organization VDC for which you want to apply security settings, and click **Configure Services**.

   The tenant portal opens Security Services.

2 Navigate to **Grouping Objects > Security Groups**

   The **Security Groups** page opens.

3 Select the security group you want to delete.

4 Click the **Delete** ( ) button.

5 To confirm the deletion, click **OK**.

The security group is deleted.

Reviewing Storage Policies

You can create and manage independent disks, and review the organization virtual data center storage policies by using the vCloud Director tenant portal.

This chapter includes the following topics:

Review Storage Policy Properties

You can review the storage policies and storage policy details.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore.
2. Under **Storage**, click **Storage Policies**.

   The list of the available storage policies displays.
3. To view the details about a storage policy, click the name of the storage policy.
4. Review the details on the **General** and **Metadata** tabs, and click **OK**.

Reviewing Virtual Data Center Properties

As an **organization administrator**, you can review the virtual data center properties.

This chapter includes the following topics:

Review Virtual Data Center Properties

You can review the properties of the virtual data centers that are assigned to your organization.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore.
2. Under **Settings**, click **General**.

You can review the properties of the virtual data center, such as name, description, and status. Metrics information about the data center includes the allocation model and vCPU, as well as CPU, and memory usage.

Review the Virtual Data Center Metadata

vCloud Director provides a general-purpose facility for associating user-defined metadata with an object. If your system administrator has created metadata for the organization virtual data center, you can review the organization data center metadata.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore.
2. Under **Settings**, click **Metadata**.

   The list of the available metadata displays.

Working with vApp Templates

A vApp template is a virtual machine image that is loaded with an operating system, applications, and data. These templates ensure that virtual machines are consistently configured across an entire organization. vApp templates are added to catalogs.

This chapter includes the following topics:

View a vApp Template

You can see the list of vApp templates that are available in the catalogs, to which you have access. You can view a vApp template and explore the virtual machines that it contains.

You can access only vApp templates that are included in catalogs items that have been shared to you. For more information about sharing catalogs, see Share a Catalog.

Prerequisites

This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **vApp Templates** from the left panel.

   The list of templates displays in a grid view.

2 (Optional) Configure the grid view to contain elements you want to see.

a From the grid view, click the grid editor icon ( ) below the list of vApp templates.

b Select the elements you want to include in the grid view, such as version, status, catalog, owner, and so on.

c Click **OK**.

The grid displays the elements you selected for each vApp template in the list.

3 To view the virtual machines included in a vApp template, click the vApp template name.

The virtual machines that the vApp template includes display in a grid.

4 (Optional) To select the elements you want to see in the grid view, click the grid editor icon ( ) below the list of virtual machines.

a Select the elements you want to include in the grid view.

b Click **OK**.

Create a vApp Template from an OVF File

You can upload an OVF package to create a vApp template in a catalog.

vCloud Director supports the Open Virtualization Format (OVF) and Open Virtualization Appliance (OVA) specifications. If you upload an OVF file that includes OVF properties for customizing its virtual machines, those properties are preserved in the vApp template. For information about creating OVF packages, see the *OVF Tool User Guide* and *VMware vCenter Converter User's Guide*

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1 From the main menu), select **Libraries**, and select **vApp Templates** from the left panel.

The list of templates displays in a grid view.

2 Click **Add**.

3 Enter a URL address to the OVF/OVA file, or click the **Upload** icon) to browse to a location accessible from your computer and select the OVF/OVA template file.

The location might be your local hard drive, a network share, or a CD/DVD drive. The supported file extensions include .ova, .ovf, .vmdk, .mf, .cert, and .strings. If you select to upload an OVF file, which references more files than you are trying to upload, for example, a VMDK file, you must browse and select all files.

4 Verify the details of the OVF/OVA template you are about to deploy and click **Next**.

5 Enter a name and, optionally a description for the vApp template, and click **Next**.

6 From the **Catalog** drop-down menu, select the catalog, to which you want to add the template.

7 Review the vApp template settings, and click **Finish**.

The new vApp template appears in the templates grid view.

Download a vApp Template

You can download a vApp template from a catalog as an OVA file to your local machine.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Libraries**, and select **vApp Templates** from the left panel.

The list of templates displays in a grid view.

2 Click the list bar (⋮) on the left of the vApp template you want to download, and select **Download**.

Note You can download vApp templates from your organization catalogs. If you are an organization administrator, you can download vApp templates from a public catalog. Otherwise, the **Download** button is dimmed.

3 (Optional) To preserve the UUIDs and MAC addresses of the virtual machines in the downloaded OVA package, select the **Preserve identity information** check box.

4 Click **OK** and wait for the download to complete.

The OVA file is saved to the default download location of your Web browser.

Delete a vApp Template

You can delete a vApp template from an organization catalog. If the catalog is published, the vApp template is also deleted from public catalogs.

Prerequisites

This operation requires the rights included in the predefined **vApp Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **vApp Templates** from the left panel.
   The list of templates displays in a grid view.
2. Click the list bar (⋮) on the left of the vApp template you want to delete, and select **Delete**.
3. Confirm the deletion.
   The deleted vApp template is removed from the grid view.

Working with Media Files

The catalog allows you to upload, copy, move, and edit the properties of media files.

This chapter includes the following topics:

Upload Media Files

You can upload new media files or new versions of existing media files to a catalog. Users with access to the catalog can open the media files with their virtual machines.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Media & Other** from the left panel.

   The list of media files displays in a grid view.

2. Click **Add**.

3. From the **Catalog** drop-down menu, select a catalog to which you want to upload the media file.

4. Enter a name for the media file.

   If you do not enter a name, the name text box is populated automatically after the name of the media file.

5. Click the upload icon ⤒) to browse and select the disk image file, for example an .iso file.

6. Click **OK**.

   After the upload starts, the media file appears in the grid.

What to do next

Depending on the file size, it might take some time for the upload to complete. You can monitor the status of the upload in the **Recent Tasks** view. For more information, see View Tasks.

Delete a Media File

You can delete media files that you no longer want to use from your catalog.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Media & Other** from the left panel.
   The list of media files displays in a grid view.
2. Click the list bar (⋮) on the left of the media file you want to delete, and select **Delete**.
3. Confirm the deletion.
   The deleted media file is removed from the grid view.

Download a Media File

You can download a media file from a catalog.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Media & Other** from the left panel.
   The list of media files displays in a grid view.
2. Click the list bar (⋮) on the left of the media file you want to download, and select **Download**.
   The download task starts, and the file is saved to the default download location of your web browser.

What to do next

Depending on the file size, it might take some time for the download to complete. You can monitor the status of the download in the **Recent Tasks** panel. For more information, see View Tasks.

Working with Catalogs

A catalog is a container for vApp templates and media files in an organization. Organization administrators and catalog authors can create catalogs in an organization. Catalog contents can be shared with other users or organizations in the vCloud Director installation or published externally for access by organizations outside the vCloud Director installation.

vCloud Director contains private catalogs, shared catalogs, and externally accessible catalogs. Private catalogs include vApp templates and media files that you can share with other users in the organization. If a system administrator enables catalog sharing for your organization, you can share an organization catalog to create a catalog accessible to other organizations in the vCloud Director installation. If a system administrator enables external catalog publishing for your organization, you can publish an organization catalog for access by organizations outside the vCloud Director installation. An organization outside the vCloud Director installation must subscribe to an externally published catalog to access its contents.

You can upload an OVF package directly to a catalog, save a vApp as a vApp template, or import a vApp template from vSphere. See Create a vApp Template from an OVF File and Save a vApp as a vApp Template to a Catalog.

Members of an organization can access vApp templates and media files that they own or that are shared with them. Organization administrators and system administrators can share a catalog with everyone in an organization or with specific users and groups in an organization. See Share a Catalog.

This chapter includes the following topics:

View Catalogs

You can access catalogs shared with you within your organization. You can access public catalogs if an organization administrator has made them accessible within your organization.

Catalog access is controlled by catalog sharing, not by the rights in your role. You can access only those catalogs or catalog items that are shared with you. For more information, see Share a Catalog.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. (Optional) Configure the grid view to contain elements you want to see.
   a. From the grid view, click the grid editor icon () displayed below the list of catalogs.
   b. Select the elements you want to include in the grid view, such as version, description, status, and so on.
   c. Click **OK**.
   The grid displays the elements you selected for each catalog.
3. (Optional) From the grid view, use the list bar (⋮) to display the actions you can take for each catalog.
   For example, you can share or delete a catalog.

Create a Catalog

You can create new catalogs and associate them with a storage policy.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. Click **New** to create a new catalog.
3. Enter the name and, optionally, a description of the catalog.
4. (Optional) Select whether you want to assign a storage policy to the catalog, and select a storage policy.

5 Click **OK**.

The new catalog appears in the grid view on the **Catalogs** tab.

Share a Catalog

You can share a catalog with all members of your organization, or with specific members.

Prerequisites

- This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.
- You must be the owner of the catalog.

Procedure

1 From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.

The list of catalogs displays in a grid view.

2 Click the list bar (⋮) on the left of the catalog you want to share, and select **Share**.

The list of users who can access the catalog appears in the grid view of the **Share Catalog** window.

3 Click **Add** to share the catalog with other users.

Option	Description
Share with everyone in this organization	Grant access to all users and groups in the organization.
Share with specific users and groups	Select the users or groups to whom you want to grant catalog access, and click **Add**.

4 Select the access level.

Option	Description
Read Only	Users with access to this catalog have read access to the vApp templates and ISO files of the catalog.
Read/Write	Users with access to this catalog have read access to the vApp templates and ISO files of the catalog and can add vApp templates and ISO files to the catalog.
Full Control	Users with access to this catalog have full control of the contents and settings of the catalog.

5 Click **OK**.

The users or groups that now have access to the catalog appear in the grid view of the **Share Catalog** dialog box.

6 (Optional) Select to share read-only access to the administrators of all other organizations

7 Click **Save**.

On the **Catalogs** tab, the Shared status for this catalog in the grid view changes.

Delete a Catalog

You can delete a catalog from your organization.

Prerequisites

This operation requires the rights included in the predefined **Catalog Author** role or an equivalent set of rights.

Note The catalog must not contain any vApp templates or media files. You can move these items to a different catalog or delete them.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. Click the list bar (⋮) on the left of the catalog you want to delete, and select **Delete**.
3. Confirm the deletion.
   The deleted catalog item is removed from the grid view.

Manage Metadata for a Catalog

As an **organization administrator** or a **catalog owner**, you can create or update the metadata for the catalogs that you own.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. Click the list bar (⋮) on the left of a catalog, and select **Metadata**.
   The metadata for the selected catalog is displayed in a grid view.
3. (Optional) To add metadata, click **Add**.
   a. Enter the metadata name.
      The name must be unique within the metadata names attached to this object.
   b. Select the metadata type, such as **Text**, **Number**, **Date and Time**, or **Yes or No**.
   c. Enter the metadata value.
   d. Click **Save**.

4 (Optional) Update existing metadata.

You cannot update the metadata name.

a Update the metadata type.

b Enter the new metadata value.

c Click **Save**.

5 (Optional) Delete existing metadata.

a Click the delete icon.

b Click **Save**.

Publish a Catalog

If the **system administrator** has granted you catalog access, you can publish a catalog externally to make its vApp templates and media files available for subscription by organizations outside the vCloud Director installation.

Prerequisites

Verify that the **system administrator** enabled external catalog publishing for the organization and granted you catalog access.

Procedure

1 From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.

The list of catalogs displays in a grid view.

2 Click the list bar (⋮) on the left of the catalog you want to publish, and select **Publish Settings**.

3 Select **Enable Publishing** and, optionally, enter a password for catalog access.

Only ASCII characters are supported.

4 Click **Save**.

Subscribe to an External Catalog

You can subscribe to an external catalog and thus create a read-only copy of an externally published catalog. You cannot modify a subscribed catalog.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- The **system administrator** must grant your organization permission to subscribe to external catalogs.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. Click **New** to create a new catalog.
3. Enter the name and, optionally, a description of the catalog.
4. Select to subscribe to an external catalog and provide the subscription URL.
5. Enter the optional password to access the catalog.
6. Select whether you want to automatically download the content from the external catalog.
7. Click **OK**.

Update the Location URL and the Password for a Subscribed Catalog

After you create a subscribed catalog, you can update the location URL and the password for the subscribed catalog.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- You must have created a subscribed catalog.
- The **system administrator** must grant your organization permission to subscribe to external catalogs.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.
   The list of catalogs displays in a grid view.
2. Click the list bar (⋮) on the left of a subscribed catalog, and select **Subscribe settings**.
   If the catalog is not a subscribed one, the option is dimmed.
3. Update the location URL and the password for this subscribed catalog.
4. Select whether you want to download the content from the external catalog automatically.
5. Click **Save**.

Synchronize a Subscribed Catalog

After you create a subscribed catalog, you can synchronize it with the original catalog to see if there are any changes. For example, if the metadata of the original catalog is changes, when you perform the synchronization, the metadata of the subscribed catalog is updated.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- You must have created a subscribed catalog.
- The **system administrator** must grant your organization permission to subscribe to external catalogs.

Procedure

1. From the main menu ☰), select **Libraries**, and select **Catalogs** from the left panel.

   The list of catalogs displays in a grid view.

2. Click the list bar (⋮) on the left of a subscribed catalog, and select **Sync**.

   If the catalog is not a subscribed one, the option is dimmed.

   The subscribed catalog is synchronized with the original one.

Working with Organization Virtual Data Center Templates

As an organization administrator or any role that has rights to view and instantiate organization virtual data center templates, you can create additional organization virtual data centers.

An organization virtual data center template specifies a configuration for an organization virtual data center and organization virtual data center network. System administrators can enable organization administrators to create these resources in their organizations by creating organization virtual data center templates and sharing them with those organizations.

By creating and sharing virtual data center templates, system administrators enable self-service provisioning of organization virtual data centers while retaining administrative control over allocation of system resources, such as provider virtual data centers and external networks.

System administrators create organization virtual data center templates and provide different organizations with access to the templates by using the vCloud Director Web interface. See *Managing Organization Virtual Data Center Templates* from the *vCloud Director Administrator's Guide*. If your organization has been provided with access to virtual data center templates, you can use the vCloud Director tenant portal to create virtual data centers from the available templates.

This chapter includes the following topics:

View Available Virtual Data Center Templates

You can view the organization virtual data center templates that a system administrator has created for you.

View the virtual data center templates before you create a new organization virtual data center from the virtual data center template.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or a role that has rights to view and instantiate organization virtual data center templates.

Procedure

- From the main menu (☰), select **Libraries**, and select **VDC Templates** from the left panel.

  The list of virtual data center templates displays in a grid view.

What to do next

Review the descriptions of the organization virtual data center templates and select the template from which you want to create a new organization virtual data center.

Create a Virtual Data Center from a Template

You can create an organization virtual data center from a virtual data center template that your system administrator has created.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or a role that has rights to view and instantiate organization virtual data center templates.

Procedure

1. From the main menu ☰), select **Libraries**, and select **VDC Templates** from the left panel.

   The list of virtual data center templates displays in a grid view.
2. Select a template, and click **New VDC**.
3. Enter a name of the virtual data center and, optionally, a description.
4. Click **Create**.

The creation of the new organization virtual data center is instantiated and might take a few minutes. You can see the progress of the task in the **Recent Tasks** panel.

What to do next

You can manage your newly created organization virtual data center by creating virtual machines, vApps, managing the network and security settings, and so on.

Managing Users, Groups and Roles

You can add organization administrators to vCloud Director individually, or as part of an LDAP group. You can also add and modify the roles that determine what rights a user has within their organization.

Important You must be an **organization administrator** to manage the users, groups, and roles within your organization. Your **system administrator** can publish one or more global tenant roles to your tenant, and as an **organization administrator**, you can see them in the list of roles. Such roles are for example, **Catalog Author**, **vApp Author**, **vApp User**, **Organization Administrator**, and so on. You cannot modify the predefined global tenant roles, but you can create and update similar custom tenant roles and assign them to users within your tenant.

This chapter includes the following topics:

Managing Users

From the tenant portal you can create, edit, import, and delete users. In addition, you can also unlock user accounts in case a user tried to log in with an incorrect password and as a result has locked their own user account.

Create a User

You can create a user within your vCloud Director organization.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.

2 In the left panel under **Access Control**, click **Users**.

The list of users is displayed.

3 Click **Create**.

4 (Optional) Enter a user name and the password setting of the user.

The minimum password length is six characters.

5 Select whether to enable the user upon creation.

6 Choose the role that you want to assign to the user.

The **Available roles** menu consist of a list of predefined roles and any custom roles that you or the system administrator might have created.

Predefined role	Description
vApp Author	The rights associated with the predefined **vApp Author** role allow a user to use catalogs and create vApps.
Console Access Only	The rights associated with the predefined **Console Access Only** role allow a user to view virtual machine state and properties and to use the guest OS.
vApp User	The rights associated with the predefined **vApp User** role allow a user to use existing vApps.
Organization Administrator	A user with the predefined **Organization Administrator** role can use the vCloud Director tenant portal or the vCloud API to manage users and groups in their organization and assign them roles, including the predefined **Organization Administrator** role. An **organization administrator** can use the vCloud API to create or update role objects that are local to the organization. Roles created or modified by an **organization administrator** are not visible to other organizations.
Defer to Identity Provider	Rights associated with the predefined **Defer to Identity Provider** role are determined based on information received from the user's OAuth or SAML Identity Provider. To qualify for inclusion when a user is assigned the **Defer to Identity Provider** role, a role name supplied by the Identity Provider must be an exact, case-sensitive match for a role, or name defined in your organization.
Catalog Author	The rights associated with the predefined **Catalog Author** role allow a user to create and publish catalogs.

7 (Optional) Enter the contact information, such as name, email address, phone number, and instant messaging ID.

8 (Optional) Enter virtual machine quota for the user.

The quota determines how many virtual machines and running virtual machines the user can manage. Select **Unlimited** if you want to provide the user with an unlimited number of virtual machines.

9 Click **Save**.

Import Users

You can add users to your organizations, by importing an LDAP user or a vCenter Single Sign-On user

and assigning them a certain role.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- Verify that you have a valid connection to an LDAP server or have vCenter Single Sign-On enabled. For information, see *vCloud Director Administrator's Guide*.

Procedure

1. From the main menu ☰), select **Administration**.
2. In the left panel under **Access Control**, click **Users**.

   The list of users is displayed.
3. Click **Import Users**.
4. Select a source from which you want to import the users.

   If you have only an LDAP server or only vCenter Single Sign-On configured, you can only view the source.

Source	Action
LDAP	Import users from an LDAP server. a Enter a full or partial name in the text box and click **Search**. b Select the users whom you want to import and click **Add**.
vCenter Single Sign-On	Import users from a vCenter Single Sign-On domain. Enter the user names of the users whom you want to import and click **Add**. The imported user names must be in User Principal Name (UPN) format, for example jdoe@mydomain.com. Separate multiple users by entering their names on separate lines.

5. Select the role which you want to assign to the users that you import.
6. Click **Save**.

Modify a User

As an organization administrator, you can modify the password, the contact, and the virtual machine quota settings of an existing user. In addition, you can also change the role of the user.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. In the left panel under **Access Control**, click **Users**.

The list of users is displayed.

3 Click the radio button next to the name of the user that you want to edit and click **Modify**.

4 Update the settings you want to modify.

a Change the password as necessary.

b Select whether to enable or disable the user.

c Update the user role.

d Update the contact information, such as name, email address, phone number, and instant messaging ID.

e Edit virtual machine quota for the user.

5 Click **Save**.

Disable or Enable a User Account

You can disable a user account to prevent that user from logging in to vCloud Director. To delete a user, you must first disable their account.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 In the left panel under **Access Control**, click **Users**.

The list of users is displayed.

3 To disable a user account, click the radio button next to the user name, click **Disable**, and confirm that you want to disable the account.

4 To enable a user account that you have already disabled, click the radio button next to the user name, and click **Enable**.

Delete a User

You can remove a user from the vCloud Director organization by deleting the user account.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- Disable the account you want to delete.

Procedure

1. From the main menu ☰), select **Administration**.

2. In the left panel under **Access Control**, click **Users**.

   The list of users is displayed.

3. Click the radio button next to the name of the user that you want to delete and click **Delete**.

4. To confirm that you want to delete the user account, click **OK**.

Unlock a Locked Out User Account

In case you have enabled a lockout policy in your vCloud Director organization, a user account is locked after a certain number of invalid login attempts. You can unlock the locked user account. Best practice is to change the password of the user and unlock the account.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.

2. In the left panel under **Access Control**, click **Users**.

   The list of users is displayed.

3. Click the radio button next to the user name, click **Unlock**.

Managing Groups

If you have a valid connection to an LDAP server or have vCenter Single Sign-On enabled you can import an LDAP group, or a vCenter Single Sign-On group. You can also edit or delete an imported group.

Import a Group

To add a group of users, you can import an LDAP group, or a vCenter Single Sign-On group.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- Verify that you have a valid connection to an LDAP server or have vCenter Single Sign-On enabled. For information, see *vCloud Director Administrator's Guide*.

Procedure

1. From the main menu ☰), select **Administration**.

2. In the left panel under **Access Control**, click **Groups**.

The list of user groups is displayed.

3 Click **Import Group**.

4 Select a source from which you want to import the user group.

If you have only an LDAP server or only vCenter Single Sign-On configured, you can only view the source.

Source	Action
LDAP	Import users from an LDAP server. a Enter a full or partial name in the text box and click **Search**. b Select the users whom you want to import and click **Add**.
vCenter Single Sign-On	Import a group from a vCenter Single Sign-On domain. Enter the group names of the groups whom you want to import and click **Add**. Separate multiple groups by entering their names on separate lines.

5 Select the role which you want to assign to the group of users that you import.

6 Click **Save**.

Delete a Group

You can remove a group from your vCloud Director organization by deleting their LDAP group.

When you delete an LDAP group, users who have a vCloud Director account based solely on their membership in that group are stranded and cannot log in.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 In the left panel under **Access Control**, click **Groups**.

The list of user groups is displayed.

3 Click the radio button next to the name of the group that you want to delete, and click **Delete**.

4 To confirm that you want to delete the group, click **OK**.

Edit a Group

You can edit a group from the vCloud Director tenant portal.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. In the left panel under **Access Control**, click **Groups**.

   The list of user groups is displayed.
3. Click the radio button next to the name of the group that you want to delete, and click **Edit**.
4. Edit the group as necessary.
   a. Change the description.
   b. Change the role of the members of the group as necessary.
5. Click **Save**.

Roles and Rights

vCloud Director uses roles and rights to determine what actions a user can perform in an organization. vCloud Director includes a number of predefined roles with specific rights.

System administrators and **organization administrators** must assign each user or group a role. The same user can have a different role in different organizations. **System administrators** can create roles and modify existing ones for the whole system, while **organization administrators** can create and modify roles only for the organization that they administer.

The vCloud Director tenant portal allows **organization administrators** to manage the roles in their organization. If a **system administrator** publishes one or more predefined tenant roles to your organization, as an **organization administrator** you can see these roles, but you cannot modify them. You can, however, create custom tenant roles with similar rights and assign them to the users within your organization.

For information about the predefined roles and their rights, see Predefined Roles and Their Rights.

Predefined Roles and Their Rights

Each vCloud Director predefined role contains a default set of rights required to perform operations included in common workflows. By default, all predefined global tenant roles are published to every organization in the system.

Predefined Provider Roles

By default, the provider roles that are local only to the provider organization are the **System Administrator** and **Multisite System** roles. **System administrators** can create additional custom provider roles.

System Administrator	The **System Administrator** role exists only in the provider organization. The **System Administrator** role includes all rights in the system. The **System administrator** credentials are established during installation and configuration. A **System Administrator** can create additional system administrator and user accounts in the provider organization.
Multisite System	Used for running the heartbeat process for multisite deployments. This role has only a single right, **Multisite: System Operations**, which gives a permission to make a vCloud API request that retrieves the status of the remote member of a site association.

Predefined Global Tenant Roles

By default, the predefined global tenant roles and the rights they contain are published to all organizations. **System Administrators** can unpublish rights and global tenant roles from individual organizations. **System Administrators** can edit or delete predefined global tenant roles. **System administrators** can create and publish additional global tenant roles.

Organization Administrator	After creating an organization, a **System Administrator** can assign the role of **Organization Administrator** to any user in the organization. A user with the predefined **Organization Administrator** role can use the vCloud Director Web Console, tenant portal, or vCloud OpenAPI to manage users and groups in their organization and assign them roles, including the predefined **Organization Administrator** role. Roles created or modified by an **Organization Administrator** are not visible to other organizations.
Catalog Author	The rights associated with the predefined **Catalog Author** role allow a user to create and publish catalogs.
vApp Author	The rights associated with the predefined **vApp Author** role allow a user to use catalogs and create vApps.
vApp User	The rights associated with the predefined **vApp User** role allow a user to use existing vApps.

Console Access Only The rights associated with the predefined **Console Access Only** role allow a user to view virtual machine state and properties and to use the guest OS.

Defer to Identity Provider Rights associated with the predefined **Defer to Identity Provider** role are determined based on information received from the user's OAuth or SAML Identity Provider. To qualify for inclusion when a user or group is assigned the **Defer to Identity Provider** role, a role or group name supplied by the Identity Provider must be an exact, case-sensitive match for a role or group name defined in your organization.

- If the user is defined by an OAuth Identity Provider, the user is assigned the roles named in the roles array of the user's OAuth token.
- If the user is defined by a SAML Identity Provider, the user is assigned the roles named in the SAML attribute whose name appears in the RoleAttributeName element, which is in the SamlAttributeMapping element in the organization's OrgFederationSettings.

If a user is assigned the **Defer to Identity Provider** role but no matching role or group name is available in your organization, the user can log in to the organization but has no rights. If an Identity Provider associates a user with a system-level role such as **System Administrator**, the user can log in to the organization but has no rights. You must manually assign a role to such users.

Except the **Defer to Identity Provider** role, each predefined role includes a set of default rights. Only a **System Administrator** can modify the rights in a predefined role. If a **System administrator** modifies a predefined role, the modifications propagate to all instances of the role in the system.

Rights in Predefined Global Tenant Roles

Various rights are common to multiple predefined global roles. These rights are granted by default to all new organizations, and are available for use in other roles created by the **Organization Administrator**.

Table 13-1. Rights Included in the Global Tenant Roles in vCloud Director

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
Catalog: Add a vApp from My Cloud	X	X	X		
Catalog: Allow External Publishing / Subscriptions for the Catalogs	X	X			
Catalog: Change Owner	X				
Catalog: Create / Delete a Catalog	X	X			
Catalog: Edit Catalog Properties	X	X			
Catalog: Share a Catalog to Other Organizations	X	X			

Table 13-1. Rights Included in the Global Tenant Roles in vCloud Director (Continued)

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
Catalog: Share a Catalog to Users / Groups within Current Organization	X	X			
Catalog: View Private and Shared Catalogs within Current Organization	X	X	X		
Catalog: View Shared Catalogs from Other Organizations	X		X		
Catalog Item: Add to My Cloud	X	X	X	X	
Catalog Item: Copy / Move a vApp Template / Media	X	X	X		
Catalog Item: Create / Upload a vApp Template / Media	X	X	X		
Catalog Item: Edit vApp Template / Media	X	X			
Catalog Item: Enable vApp Template / Media Download	X	X	X		
Catalog Item: View vApp Templates / Media	X	X	X	X	
Custom Entity: View All Custom Entity Instances in Organization	X				
Custom Entity: View Custom Entity Instance	X				
Disk: Change Owner	X	X			
Disk: Create a Disk	X	X	X		
Disk: Delete a Disk	X	X	X		
Disk: Edit Disk Properties	X	X	X		
Disk: View Disk Properties	X	X	X	X	
Distributed Firewall: Configure Distributed Firewall Rules	X				
Distributed Firewall: View Distributed Firewall Rules	X				
Gateway: Configure Syslog Server	X				
Gateway: Convert to Advanced Gateway	X				
Gateway: View Gateway	X				
Gateway Services: DHCP Configure	X				
Gateway Services: Firewall Configure	X				
Gateway Services: IPSEC VPN Configure	X				
Gateway Services: Load Balancer Configure	X				
Gateway Services: NAT Configure	X				

Table 13-1. Rights Included in the Global Tenant Roles in vCloud Director (Continued)

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
Gateway Services: Static Routing Configure	X				
General: Administrator Control	X				
General: Administrator View	X				
General: Send Notification	X				
Hybrid Tunnel: Acquire Control Ticket	X				
Hybrid Tunnel: Acquire From-the-Cloud Tunnel Ticket	X				
Hybrid Tunnel: Acquire To-the-Cloud Tunnel Ticket	X				
Hybrid Tunnel: Create From-the-Cloud Tunnel	X				
Hybrid Tunnel: Create To-the-Cloud Tunnel	X				
Hybrid Tunnel: Delete From-the-Cloud Tunnel	X				
Hybrid Tunnel: Delete To-the-Cloud Tunnel	X				
Hybrid Tunnel: Update From-the-Cloud Tunnel Endpoint Tag	X				
Hybrid Tunnel: View From-the-Cloud Tunnel	X				
Hybrid Tunnel: View To-the-Cloud Tunnel	X				
Network: Edit Properties					
Network: View Properties					
Organization: Allow Access to All Organization VDCs	X				
Organization: Edit Access Control List of Organization VDCs	X				
Organization: Edit Federation Settings	X				
Organization: Edit Leases Policy	X				
Organization: Edit Organization Associations	X				
Organization: Edit Organization Network Properties	X				
Organization: Edit Organization OAuth Settings	X				
Organization: Edit Organization Properties	X				
Organization: Edit Password Policy	X				
Organization: Edit Quotas Policy	X				

Table 13-1. Rights Included in the Global Tenant Roles in vCloud Director (Continued)

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
Organization: Edit SMTP Settings	X				
Organization: Implicitly Import User/Group from IdP while Editing VDC ACL	X				
Organization: View Access Control List of Organization VDCs	X				
Organization: View Catalog ACL	X	X			
Organization: View Organization Networks	X				
Organization: View Organizations	X	X	X		
Organization: View vApp ACL	X		X		
Organization vDC: Edit Organization VDC Name and Description	X				
Organization vDC: Edit VM-VM Affinity Rule	X	X	X		
Organization vDC: Manage Firewall	X				
Organization vDC: Set Default Storage Policy	X				
Organization vDC: View Compute Policies for an Organization VDC	X		X	X	
Organization vDC: View Organization VDCs	X				
Role: Create / Update / Delete a Role	X				
Service Library: View Services Making Up the Service Library	X				
User: View Group / User	X				
VCD Extension: View Tenant Portal Plugin Information	X	X	X	X	
VDC Template: Instantiate Organization VDC Templates	X				
VDC Template: View Organization VDC Templates	X				
VM Monitoring: View historic metrics for the Organization	X				
VM Monitoring: View historic metrics for the Organization VDC	X				
vApp: Access to VM Console	X	X	X	X	X
vApp: Allow Metadata Mapping Domain to vCenter Server	X	X	X		
vApp: Change Owner	X				
vApp: Change vApp Template Owner	X	X			

Table 13-1. Rights Included in the Global Tenant Roles in vCloud Director (Continued)

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
vApp: Copy a vApp	X	X	X	X	
vApp: Create / Reconfigure vApp	X	X	X		
vApp: Create / Revert / Remove / a Snapshot	X	X	X	X	
vApp: Delete a vApp	X	X	X	X	
vApp: Download a vApp	X	X	X		
vApp: Edit / View VM Boot Options	X	X	X		
vApp: Edit VM CPU	X	X	X		
vApp: Edit VM Hard Disk	X	X	X		
vApp: Edit VM Memory	X	X	X		
vApp: Edit VM Network	X	X	X	X	
vApp: Edit VM Properties	X	X	X	X	
vApp: Edit vApp Properties	X	X	X	X	
vApp: Manage VM Password Settings	X	X	X	X	X
vApp: Share a vApp	X	X	X	X	
vApp: Start / Stop / Suspend / Reset a vApp	X	X	X	X	
vApp: Upload a vApp	X	X	X		
vApp: View VM metrics	X		X	X	

Create a Custom Tenant Role

Organization administrators can use the tenant portal to create custom tenant role objects in the organizations they administer.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. In the left panel under **Access Control**, click **Roles**.

   The list of roles is displayed.
3. Click **Add**.
4. Enter a name and, optionally, a description of the role.

5 Expand the rights for the role and select the rights for the role.

The rights are grouped in categories and subcategories that allow either viewing or managing objects.

Option	Description
Access Control	Rights controlling the access to view and manage certain objects.
Administration	Rights controlling the administrative access.
Compute	Rights controlling access and management of the organization and provider virtual data centers, the vApps, organization virtual data centers templates, virtual machine groups, and virtual machine monitoring.
Extensions	Rights controlling the access to any additional plug-ins and vCloud Director extensions.
Infrastructure	Rights controlling the access and management of the infrastructure objects, such as datastores, disks, hosts, and so on.
Libraries	Rights controlling access and management of any catalogs and catalog items.
Networking	Rights controlling access and management of the network settings.

6 Click **Save**.

Edit a Custom Tenant Role

Organization administrators can use the tenant portal to edit custom tenant role objects in the organizations they administer. As an organization administrator you can only view the global tenant roles that a system administrator has published to your organization. You cannot edit global tenant roles.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 In the left panel under **Access Control**, click **Roles**.

The list of roles is displayed.

3 Click the radio button next to the role that you want to edit, and click **Edit**.

4 Modify the role settings as needed.

a Change the name and, optionally, the description of the role.

b Edit the rights for the role.

5 Click **Save**.

Delete a Role

Organization administrators can use the tenant portal to delete role objects in the organizations they administer.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. In the left panel under **Access Control**, click **Roles**.

   The list of roles is displayed.
3. Click the radio button next to the role that you want to delete, and click **Delete**.
4. Confirm that you want to delete the role by clicking **OK**.

Enable Your Organization to Use a SAML Identity Provider

Enable your organization to use a Security Assertion Markup Language (SAML) identity provider, also called single sign-on, to import users and groups from a SAML identity provider and allow imported users to sign on to the organization with the credentials established in the SAML identity provider.

When you import users and groups, the system extracts a list of attributes from the SAML token, if available, and uses them for interpreting the corresponding pieces of information about the user attempting to log in.

- email address = "EmailAddress"
- user name = "UserName"
- full name = "FullName"
- user's groups = "Groups"
- user's roles = "Roles"

  The role attribute is configurable.

Group information is necessary if the user is not directly imported but is expected to be able to log in by virtue of membership in imported groups. A user might belong to multiple groups, and can have multiple roles during a session.

If an imported user or group is assigned the **Defer to Identity Provider** role, the roles are assigned based on the information gathered from the Roles attribute in the token. If a different attribute is used, this attribute name can be configured by using the API only, and only the Roles attribute is configurable. If the **Defer to Identity Provider** role is used, but no role information can be extracted, the user can log in but does not have any rights to perform any activities.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- Verify that you have access to an OpenAM or Active Directory Federation Services SAML identity provider.
- Verify that your system has updated JCE-unlimited strength jurisdiction policy files. See *Install Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files* in the *vCloud Director Administrator's Guide*.

- Make sure that you receive the required metadata from your SAML identity provider. You must import the metadata to vCloud Director either manually or as an XML file. The metadata must include the following information:
  - The location of the single sign-on service
  - The location of the single logout service
  - The location of the service's X.509 certificate

  For information on configuring and acquiring metadata from an OpenAM or Active Directory Federation Services SAML provider, see the documentation for your SAML identity provider.

Procedure

1. From the main menu ☰), select **Administration**.
2. Under **Identity Providers**, click **SAML**.
3. Click **Edit**.
4. On the **Service Provider** tab, enter the Entity ID.

   The Entity ID is the unique identifier of your organization to your identity provider. You can use the name of your organization, or any other string that satisfies the requirements of your SAML identity provider.

   Important Once you specify an Entity ID, you cannot delete it. To change the Entity ID, you must do a full SAML reconfiguration for your organization. For information about Entity IDs, see Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) 2.0.
5. Click the **Metadata** link to download the SAML metadata for your organization.

   The downloaded metadata must be provided as-is to your identity provider.
6. Review the Certificate Expiration date and, optionally, click **Regenerate** to regenerate the certificate used to sign federation messages.

   The certificate is included in the SAML metadata, and is used for both encryption and signing. Either or both encryption and signing might be required depending on how trust is established between your organization and your SAML identity provider.
7. On the **Identity Provider** tab, enable the **Use SAML Identity Provider** toggle.
8. Copy and paste the SAML metadata you received from your identity provider to the text box, or click **Upload** to browse to and upload the metadata from an XML file.
9. Click **Save**.

What to do next

- Configure your SAML provider with vCloud Director metadata. See your SAML identity provider documentation and the *vCloud Director Installation and Upgrade Guide*.

- Import users and groups from your SAML identity provider. See Chapter 13 Managing Users, Groups and Roles

Managing Your Organization

As an **organization administrator**, you can modify a number of settings within your organization, such as name of the organization, email settings, domain settings, metadata, policies, and so on.

This chapter includes the following topics:

Edit the Organization Name and Description

You can edit the full name and the description of your organization.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. Under **Settings**, click **General**.

   The list of general settings, such as organization name, default URL, full name, and description displays.

3 To modify the full name and the description of the organization, click **Edit**.

4 Apply the necessary changes and click **Save**.

Modify Your Email Settings

You can review and modify the default email settings that were set when the system administrator created your organization

vCloud Director sends alert emails when having important information to report, for example, when a data store is running out of space. By default, an organization sends email alerts to the system administrators or a list of email addresses specified at the system level by using an SMTP server specified at the system level. You can modify the email settings at the organization level if you want vCloud Director to send alerts for that organization to a different set of email addresses than those specified at the system level or you want the organization to use a different SMTP server to send alerts than the server specified at the system level.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 Under **Settings**, click **Email**.

The email settings for your organization are displayed.

3 Click **Edit**.

4 Edit the SMTP server settings on the **SMTP Server** tab.

a Select whether to use a custom SMTP server or the default.

b If you select to use a custom SMTP server, enter the DNS host name or IP address of the SMTP server in the **SMTP server name** text box.

c (Optional) Enter the SMTP server port.

d (Optional) Select whether to require authentication and enter a user name and password.

5 To edit the notification settings, click the **Notification Settings** tab.

a Select to use custom notification settings.

b Enter the email address that appears as the sender for organization emails.

c (Optional) Enter the text to use as the email subject prefix.

d (Optional) Select whether to send notifications to all organization administrators or to specific email addresses.

e (Optional) If you select to send notifications to specific email addresses, enter the email addresses by separating them with a comma.

6 Click **Save**.

Test SMTP Settings

After you modify the email settings for your organization, you can test the SMTP settings.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 Under **Settings**, click **Email**.

The email settings for your organization are displayed.

3 Click **Test**.

4 Enter a destination email address and the SMTP server password to test the SMTP settings, and click the **Test** button.

Modify Domain Settings for the Virtual Machines in Your Organization

You can set a default Windows domain which virtual machines created in your organization can join. Virtual machines can always join a domain for which they have credentials, regardless of whether you specify a default domain or not.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1 From the main menu ☰), select **Administration**.

2 Under **Settings**, click **Guest Personalization**.

3 Select to enable the domain join for the virtual machines in the organization.

4 Enter the domain name, user name, and password.

The credentials that you enter apply to a regular domain user, not a domain administrator.

5 (Optional) Enter an account organizational unit.

6 Click **Save**.

Configure and Manage Multisite Deployments

After a **system administrator** has associated two sites, **organization administrators** at any member site can begin associating their organizations.

To create an association between two organizations (we will call them Org-A and Org-B here), you must be an **organization administrator** for both organizations so that you can log in to each organization, retrieve its local association data, and submit the retrieved data to the other organization.

Important The process of associating two organizations can be logically decomposed into two complementary pairing operations. The first operation (in this example) pairs Org-A at Site-A with Org-B at Site-B. You must then pair Org-B at Site-B with Org-A at Site-A. Until both pairings are complete, the association is incomplete.

Prerequisites

- The sites occupied by the organizations must be associated.
- You must be a **system administrator** at both sites or an **organization administrator** at both organizations.

Procedure

1 Log in to the vCloud Director tenant portal of Org-A at Site-A to retrieve its local association data.
   a Click **Administration**.
   b Under **Settings**, click **Multisite**.
   c To download the data in XML format, click **Export local association data**.
      The browser saves the data in a file in its Downloads folder.

2 Log in to the vCloud Director tenant portal of Org-B at Site-B to submit the local association data from Org-A at Site-A.
   a Click **Administration**.
   b Under **Settings**, click **Multisite**.

c Click **Create new organization association**.

Submit the association data you downloaded in Step 1 to Org-B by clicking the upload arrow below the **New Association XML** text box and selecting the local association data you downloaded in Step 1.

d Click **Next** to verify and submit the data.

The system pairs Org-A at Site-A with Org-B at Site-B.

e Click **Finish** to view the associated organization.

f To view details of the associated organization or delete the association, click the **Organization Name** card.

3 Complete the association by repeating Step 1 and Step 2 to retrieve the local association data from Org-B and submit it to Org-A.

Understanding Leases

Creating an organization involves specifying leases. Leases provide a level of control over an organization's storage and compute resources by specifying the maximum amount of time that vApps can be running and that vApps and vApp templates can be stored.

The goal of a runtime lease is to prevent inactive vApps from consuming compute resources. For example, if a user starts a vApp and goes on a vacation without stopping it, the vApp continues to consume resources.

A runtime lease begins when a user starts a vApp. When a runtime lease expires, vCloud Director stops the vApp.

The goal of a storage lease is to prevent unused vApps and vApp templates from consuming storage resources. A vApp storage lease begins when a user stops the vApp. Storage leases do not affect running vApps. A vApp template storage lease begins when a user adds the vApp template to a vApp, adds the vApp template to a workspace, downloads, copies, or moves the vApp template.

When a storage lease expires, vCloud Director marks the vApp or vApp template as expired, or deletes the vApp or vApp template, depending on the organization policy you set.

Modify the vApp and vApp Template Lease Policies Within Your Organization

You can review and modify the default policies that were set by the system administrator when your organization was created.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. Under **Settings**, click **Policies**.

   You can view the default policies that your system administrator has set.
3. Click **Edit**.
4. Edit the vApp leases.

   vApp leases provide a level of control over the organization storage and compute resources by specifying the maximum amount of time that vApps can be running and that vApps can be stored. You can also specify what happens to the vApps when their storage lease expires.

   a. To define how long vApps can run before they are automatically stopped, enter the maximum runtime lease.

   b. Select a runtime expiry action, such as power off or suspend.

   c. To define how long stopped vApps remain available before being automatically cleaned up, enter the maximum storage lease.

   d. Select a storage cleanup action, such as to delete permanently the vApps or move them to the expired items.
5. Edit the vApp template lease.

   vApp template leases provide a level of control over the organization storage and compute resources by specifying the maximum amount of time that vApp templates can be stored. You can also specify what happens to the vApp templates when their storage lease expires.

   a. To define how long the vApp templates remain available before being automatically cleaned up, enter the maximum storage lease.

   b. Select a storage cleanup action, such as to delete permanently the vApp templates or move them to the expired items.
6. Click **OK**.

Modify the Default Quotas for the Virtual Machines in Your Organization

You can review and modify the default quota policies that were set by the system administrator when your organization was created.

Quotas determine how many virtual machines each user in the organization can store and power on in the organization virtual data centers. The quotas that you specify act as the default for all new users added to the organization. Quotas set at the user level take precedence over quotas set at the organization level.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. Under **Settings**, click **Policies**.

   You can view the default policies that your system administrator has set.
3. Click **Edit**.
4. Choose between an unlimited number of virtual machines and a number that you specify.
5. Choose between an unlimited number of powered on virtual machines and a number that you specify.
6. Click **OK**.

Modify the Password and User Account Policies Within Your Organization

You can review and modify the default password and user account policies that were set by the system administrator when your organization was created.

The password and user account policies define the vCloud Director behavior when a user enters an invalid password.

Prerequisites

This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.

Procedure

1. From the main menu ☰), select **Administration**.
2. Under **Settings**, click **Policies**.

   You can view the default policies that your system administrator has set.
3. Click **Edit**.
4. Enable locking of a user account after a number of invalid login attempts.
5. Enter the number of invalid login attempts before the account is locked.
6. Enter the time interval in minutes, in which the user with locked account cannot log back in.
7. Click **OK**.

Working with Custom Entity Definitions

The custom entity definitions in vCloud Director are object types that are bound to vRealize Orchestrator object types. Users within a vCloud Director organization can own, manage, and change these types according to their needs. By executing services, organization users can instantiate the custom entities and apply actions over the instances of the objects.

This chapter includes the following topics:

Search for a Custom Entity

You can search for those of the custom entities that were published to your organization.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the **Search** text box on the top of the page, enter a word or a character of the name of the entity you want to find.

   The search results display in a card view of twelve items per page, sorted by names in alphabetical order.

Edit a Custom Entity Definition

You can modify the name and the description of a custom entity. You cannot change the type of the entity or the vRealize Orchestrator object type, to which the entity is bound, these are the default properties of the custom entity. If you want to modify any of the default properties, you must delete the custom entity definition and recreate it.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the card of the selected custom entity, select **Actions > Edit**.

   A new dialog opens.

3. Modify the name or the description of the custom entity definition.

4. Click **OK** to confirm the change.

Add a Custom Entity Definition

You can create a custom entity and map it to an existing vRealize Orchestrator object type.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. Click the + icon to add a new custom entity.

   A new dialog opens.

3 Follow the steps of the **Custom Entity Definition** wizard.

Step	
Name and Description	Enter a name and, optionally a description for the new entity. Enter a name for the entity type, for example sshHost.
vRO	From the drop-down menu, select the vRealize Orchestrator that you will use to map the custom entity definition. **Note** If you have more than one vRealize Orchestrator server, you must create a custom entity definition for each one of them separately.
Type	Click the view list icon) to browse through the available vRealize Orchestrator object types grouped by plug-ins. For example, **SSH > Host**. If you know the name of the type, you can enter it directly in the text box. For example SSH:Host.
Review	Review the details that you specified and click **Done** to complete the creation.

The new custom entity definition appears in the card view.

Custom Entity Instances

Running a vRealize Orchestrator workflow with an input parameter being an object type that is already defined as a custom entity definition in vCloud Director shows the output parameter as an instance of a custom entity.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1 From the main menu), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2 In the card of the selected custom entity, click **Instances**.

The available instances display in a grid view.

3 Click the list bar ( ) on the left of each entity to display the associated workflows.

Clicking on a workflow initiates a workflow run which takes the entity instance as an input parameter.

Associate an Action to a Custom Entity

By associating an action to a custom entity definition, you can execute a set of vRealize Orchestrator workflows on the instances of a particular custom entity.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the card of the selected custom entity, select **Actions > Associate Action**.

   A new dialog opens.

3. Follow the steps of the **Associate Custom Entity to VRO Workflow** wizard.

Step	Details
Select VRO Workflow	Select one of the listed workflows. These are the workflows that are available in the **Service Library** page.
Select Workflow Input Parameter	Select an available input parameter from the list. You associate the type of the vRealize Orchestrator workflow with the type of the custom entity definition.
Review Association	Review the details that you specified and click **Done** to complete the association.

For example, if you have a custom entity of type SSH:Host, you can associate it with the Add a Root Folder to SSH Host workflow by selecting the sshHost input parameter, which matches the type of the custom entity.

Dissociate an Action from a Custom Entity Definition

You can remove a vRealize Orchestrator workflow from the list of associated actions.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the card of the selected custom entity, select **Actions > Dissociate Action**.

   A new dialog opens.

3. Select the workflow you want to remove and click **Dissociate Action**.

   The vRealize Orchestrator workflow is no longer associated with the custom entity.

Publish a Custom Entity

You must publish a custom entity so users from other tenants or service providers can run workflows using the custom entity instances as input parameters.

Prerequisites

This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu ☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the card of the selected custom entity, select **Actions > Publish**.

   A new dialog opens.

3. Choose whether you want to publish the custom entity definition to service providers, all tenants, or only to selected tenants.

4. Click **Save** to confirm the change.

   The custom entity definition becomes available to the selected parties.

Delete a Custom Entity

You can delete a custom entity definition if the custom entity is no longer in use, if it was configured incorrectly, or if you want to map the vRealize Orchestrator type to a different custom entity.

Prerequisites-This operation requires the Custom Entity rights to be included in the predefined user role.

Procedure

1. From the main menu (☰), select **Libraries**, and under **Services** select **Custom Entity Definitions**.

   The list of custom entities displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the custom entity, the vRealize Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2. In the card of the selected custom entity, select **Actions > Delete**.

3. Confirm the deletion.

4. The custom entity is removed from the card view.