vCloud Director Tenant Portal Guide

19 SEP 2019

vCloud Director 10.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

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. You can also configure advanced networking capabilities that are provided by VMware NSX® for vSphere® within a vCloud Director environment. 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 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.

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.

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. 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.

Dedicated vCenter Server Instances (SDDCs) and Proxies

A Software-Defined Data Center (SDDC) encapsulates an entire vCenter Server environment. A dedicated vCenter Server instance can include one or more proxies that provide access to different components from the underlying environment. The **system administrator** can publish one or more dedicated vCenter Server instances to your organization. You can use the containing proxies to access the UI or API of the proxied components.

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.
Datacenter Groups	Navigates you to the **Datacenter Groups** screen for managing cross-virtual data center networks. By default, only the **system administrator** can view this menu item.
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.

Use the vCloud Director Global Search

You can use the vCloud Director global search to perform a search by a name or part of a name among the names of the objects in your environment. You can also search for a virtual machine by its IP address if the IP address of the virtual machine is static.

The list of preset objects is:

- Data centers
- vApp templates

- vApps
- Virtual machines
- vApp networks
- Catalogs

If a virtual machine uses an IP address assigned by DHCP, the search does not return its IP address. If you want to search for a virtual machine that is with an IP address assigned by DHCP, you must search by name.

By default, you can search only within the objects in your local site. If you have a multisite environment, you can search among multiple sites.

Procedure

1. In the right-upper corner of the vCloud Director tenant portal, click the **Search** () icon.
2. (Optional) Pin the search panel by clicking the **Pin** () icon.
3. In the **Search** text box, enter a symbol, a part of a name, or IP address by which to search for matching object names or static IP addresses of virtual machines.
4. If you use a multisite environment, select the sites within which you want to perform the search.
5. Press **Enter**.

The top five matching results per object type are displayed. The results are sorted alphabetically.

What to do next

- To see more results, if there are any, click **Load more** under each object type.
- To see more information about a specific object from the search results, point to the object.
- To manage a specific object, for example, to view or modify the settings of an object, click the object. The details about the object display on the left.

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.
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

2

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

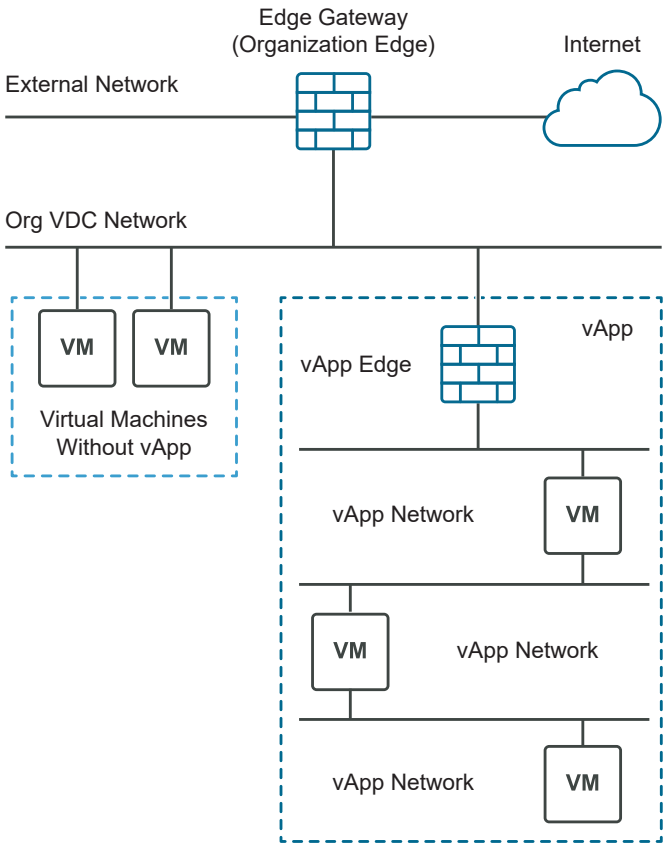
Virtual Machine Architecture

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. 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. 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.

4 (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.

5 (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.

6 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 **New VM**.

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

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

5 (Optional) Enter a meaningful description.

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

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 (Optional) Select a VM placement policy and a VM sizing policy. VM placement and VM sizing policy drop-down menus are visible only if the service provider has published such policies to the organization VDC. d (Optional) Select the size of the virtual machine from the predefined sizing options or click **Custom Sizing Options** to enter the number of virtual CPUs, cores per socket, and memory settings manually. If you select a VM sizing policy that defines the VM size, this option is not visible. The predefined sizes of the virtual machine are: **Small**, **Medium**, and **Large**. e Specify the storage settings for the virtual machine, such as storage policy and size in GB. f 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. a Select a virtual machine template from the list of available templates. b (Optional) Select a VM placement policy and a VM sizing policy. VM placement and VM sizing policy drop-down menus are visible only if the service provider has published such policies to the organization VDC. If the selected template has assigned policies, you might be limited to the predefined template policies. c (Optional) Select to use a custom storage policy and select the storage policy to use from the **Custom storage policy to use** drop-down menu. d Read and accept the end-user license agreement, if there is any.

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 VMware Remote Console download page, and select the link for your platform.

  www.vmware.com/go/download-vmrc

- On the **Virtual Datacenters** dashboard screen in the vCloud Director tenant portal, click the card of the virtual data center that you want to explore. Select a virtual machine, and from the **Actions** menu select **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 **Actions** 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 **Actions** 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 **Actions** 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 **Actions** 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 **Actions** 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 **Actions** 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 **Actions** 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 in a card view and, optionally, filter the list of virtual machines from the **Look in** drop-down menu.
3. From the **Actions** menu of the virtual machine, 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 **Actions** 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. To open the Web console of the virtual machine, from the **Actions** menu, select **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.

vCloud Director supports hardware versions depending on the backing vSphere resources. The supported hardware version depends on the latest supported virtual hardware version in the backing Provider VDC. An **Organization Administrator** or a **System Administrator** can set the hardware version to an earlier than the latest supported version by the underlying hardware. The vCloud Director tenant portal dynamically sets the list of selectable virtual hardware versions based on the backing hardware of the Organization or Provider VDC.

For information about the hardware features available with virtual machine compatibility settings, see *vSphere Virtual Machine Administration*.

For information about the VMware products and their virtual hardware version, see https://kb.vmware.com/s/article/1003746.

Prerequisites

- Stop the virtual machine or the vApp that contains the virtual machine.

- Verify that the latest version of VMware Tools is installed on 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. From the **Actions** 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	Action
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.

Option	Action
Description	Edit the 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.
Boot Delay	Specify the time in milliseconds to delay the boot operation. 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.
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 to which this virtual machine belongs.
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.
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.

Option	Description
Size	Enter the hard disk size in MB. You can increase the size of the hard disk later. **Note** You can increase the size of an existing hard disk if the virtual machine is not a linked clone and it has no snapshots.
Policy	The storage policy for the virtual machine is used by default. 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.

Option	Description
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.

6 Under **NICs**, click **Add** to add a new NIC.

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	Select this option to enable guest customization.
Change SID	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.

Option	Description
Allow local administrator password	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.
Require Administrators to change password on first login	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.
Auto generate password	Select this option to allow password auto generation.
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 by selecting an option from the **Priority** drop-down menu.

Option	Description
Low	Allocates 500 shares per virtual CPU.
Normal	Allocates 1000 shares per virtual CPU.
High	Allocates 2000 shares per virtual CPU.
Custom	Allows you to 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 by entering the reservation in MHz, 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 by selecting an option from the **Priority** drop-down menu.

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

8 Specify the reservation for the memory settings in MB 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 **Actions** menu, select **Insert Media**.
5. On 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 **Actions** 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.

When you copy a virtual machine, the snapshots are not included in the copy.

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 **Actions** 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 hyphens. It cannot consist of digits only and cannot contain spaces.
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.

When you move a virtual machine to a different vApp, the snapshots that you have taken are lost.

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 **Actions** 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 hyphens. It cannot consist of digits only and cannot contain spaces.
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 **New**.
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 **New**.

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 and click **Details**.

4 Click **Monitoring chart** to expand the monitoring view.

   The monitoring chart displays.

5

6 Select a metric option for monitoring virtual machines.

The list in the **Metric** drop-down menu varies depending on the choices of your **system administrator**. You see some or all of the options.

Metric	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.
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.

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

7 (Optional) Change the time frame for metrics collection.

8 Click **Refresh**.

9 To save your changes, click **Save**.

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 a named 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 **Actions** 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. (Optional) Select whether to snapshot the memory of the virtual machine.

   When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

   When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.

5 (Optional) Select whether to quiesce the guest file system.

This operation requires that VMware Tools is installed on the virtual machine. When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

You cannot quiesce virtual machines that have large capacity disks.

6 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 **Actions** 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 **Actions** 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 **Actions** 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 **Actions** menu of the virtual machine that you want to delete, select **Delete**.

4 Confirm the deletion.

The virtual machine is deleted.

Working with vApps

3

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:

- Download a vApp as an OVF Package
- Renew a vApp Lease
- 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 **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 hyphens. A computer name cannot consist of digits only and cannot contain spaces.

b (Optional) Enter a meaningful description.

c 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 (Optional) Select a VM placement policy and a VM sizing policy. VM placement and VM sizing policy drop-down menus are visible only if the service provider has published such policies to the organization VDC. 4 Select the size of the virtual machine or click **Custom Sizing Options** to enter the compute, memory, and storage settings manually. The predefined sizes of the virtual machine are small, medium, or large. 5 Specify the storage options such as storage policy and size in GB. 6 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. 1 Select the virtual machine template from the catalog. 2 (Optional) Select a VM placement policy and a VM sizing policy. VM placement and VM sizing policy drop-down menus are visible only if the service provider has published such policies to the organization VDC. If the selected template has assigned policies, you might be limited to the predefined template policies. 3 (Optional) Select to use a custom storage policy and select the policy from the **Custom storage policy to use**. 4 If there is an end-user license agreement available, you must review and accept it.

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

You can see the added virtual machine in the catalog.

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

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

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.
   - Select a network for each virtual machine from the **Network** drop-down menu.
   - You can select the **Switch to the advanced networking workflow** check box, and enter the network settings such as primary NIC, network adapter type, network, IP assignment and IP address settings for each virtual machine in the vApp manually.

   You can configure additional properties for virtual machines after you complete the wizard.
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.
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 On the Ready to Complete page, review your settings 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 On the **Accept Licenses** page of the wizard, read the end user license agreement and click **Accept**.

4 Click **Next**.

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

6 Specify how long this vApp can run before it is automatically stopped in hours or days.

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

8 Click **Next**.

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

10 Select a storage policy.

11 Click **Next**.

12 Select the networks to which you want each virtual machine to connect.

- Select a network for each virtual machine from the **Network** drop-down menu.
- You can select the **Switch to the advanced networking workflow** check box, and enter the network settings such as primary NIC, network adapter type, network, IP assignment and IP address settings for each virtual machine in the vApp manually.

You can configure additional properties for virtual machines after you complete the wizard.

13 Click **Next**.

14 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.
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.
Hard disk properties	Enter the size of the virtual machine hard disk in MB.

15 On the Ready to Complete page, review your settings and click **Finish**.

The new vApp appears in the card view.

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 **Actions** menu of the vApp you want to power on, select **Power On**.

The vApp is powered on.

Power off a vApp

Powering off a vApp powers off all the virtual machines in the vApp. You must power off 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 **Actions** 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.

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 **Actions** menu of the vApp you want to stop, select **Stop**.
4. Click **OK**.

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

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 **Actions** 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 **Actions** 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 **Actions** 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.
Virtual data center	The name of the data center to which the vApp belongs.
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 hours or days. Defines how long the vApp can run before it is automatically stopped. b Schedule the storage lease in number of hours or days. Defines the how long 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.
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 and select the access level. ■ To grant full control, select **Full Control**. All users in the organization 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**.
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.

Display a vApp Network Diagram

A vApp network diagram provides a graphical view of the virtual machines and networks in a vApp.

Prerequisites

To view the vApp network diagram, your vApp must contain less than 40 virtual machines. If the vApp contains more than 40 virtual machines, the diagram is not available.

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 Diagram** tab.

The diagram showing how the virtual machines and the networks in the vApp are connected is displayed. A star sign represents a primary NIC. If a NIC is connected, its color is green, if a NIC is not connected, its color is white.

5 (Optional) To highlight the connected virtual machines and networks, click a network or a virtual machine.

The connected objects and the connections between them are highlighted.

What to do next

You can add virtual machines or networks from this page.

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.

Fence a vApp Network

Powering on identical virtual machines which are included in different vApps might result in a conflict. To allow powering on of identical virtual machines in different vApps without conflicts, you must fence the vApp.

Fencing a vApp isolates the MAC and IP addresses of the virtual machines and changes the connection type of the organization VDC networks from direct to fenced. On the fenced networks firewall is automatically enabled and configured so that only outgoing traffic is allowed. When you fence a vApp, you can also configure NAT and firewall rules on the fenced networks.

Prerequisites

- You can fence only direct vApp networks. If the vApp uses more than one network and the other networks are, for example, routed, only the direct network is fenced.
- The virtual machines in the vApp that use the direct network must be stopped, so that the direct vApp network is not currently in use.

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.
5. If the vApp is not fenced, click the **Edit** button.
6. Toggle on the **Fence vApp** option and click **OK**.

The IP and MAC addresses of the virtual machines become isolated. You can power on identical virtual machines in different vApps without a conflict.

Add a 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. An edge gateway is created and attached to the isolated network and the organization virtual data center network. Traffic going to and from the virtual machines pass through the edge gateway, which translates the IP address using NAT and proxy-AR. 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 **Actions** 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 of available networks.
vApp Network	a Enter a name and, optionally, a description for the network. b Enter the network gateway CIDR. 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. f (Optional) To be able to connect to an organization virtual data center network, toggle on the **Connect to an organization VDC network** option and select a network from the list.

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. On the **Networks** tab, select the network that you want to delete, click **Delete**, and confirm the deletion.

Working 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 instead 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 a named 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 **Actions** 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. (Optional) Select whether to snapshot the memory of the vApp.

   When you capture the vApp memory state, the snapshot retains the live state of the vApp and the virtual machines in the vApp. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

   When you capture the memory state, the vApp's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the vApp and the disks are crash consistent unless you quiesce them.
5. (Optional) Select whether to quiesce the guest file system.

   This operation requires that VMware Tools is installed on the virtual machines in the vApp. When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

   You cannot quiesce vApps that have large capacity disks.
6. 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 **Actions** 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 **Actions** menu of the vApp for which you want to remove a snapshot, select **Remove Snapshot**.

4 Click **OK**.

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 **Actions** 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 **Actions** menu of the vApp you want to move, select **Move to**.

4 Select the virtual data center where you want to move the vApp and click **OK**.

5 (Optional) Select the storage policy.

6 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 **Actions** 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 (Optional) Select a storage policy.

7 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 **Actions** 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 (Optional) 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 **Actions** 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 hyphens. A computer name cannot consist of digits only and cannot contain spaces.
6. (Optional) Enter a meaningful description.
7. Select whether you want the virtual machine to power on right after it is created.

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 compute policy. d Select the size of the virtual machine or click **Custom Sizing Options** to enter the compute, memory, and storage settings manually. The predefinded sizing options are small, medium, or large. e Specify the storage settings of the virtual machine, such as storage policy and size in GB. f 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. a Select the virtual machine template from the catalog. b (Optional) Select to use a custom storage policy and select the policy from the **Custom storage policy to use**. c If there is an end user license agreement available, you must review and accept it.

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

10 Click **Add** to add the virtual machine to the vApp.

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 **Actions** 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 or as an OVA, which is a single file distribution of the same OVF file 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 **Actions** menu of the vApp that you want to download, select **Download**.

4 Select the format in which you want to download the vApp.

5 (Optional) Select **Preserve identity information** to include the UUIDs and MAC addresses of the virtual machines that reside in the vApp in the downloaded OVF package.

This limits the portability of the package and must be used only when necessary.

6 Click **OK** to confirm the selection and start the download.

By default, the package is downloaded in the `Downloads` folder for your browser.

Renew a vApp Lease

If the lease of a vApp has expired, or it is about to expire, you can renew it.

Prerequisites

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 **vApps** from the left panel.

2 Select the vApp you want to renew.

3 From the **Actions** 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 **Actions** menu, select **Delete**.

4 Click **OK**.

The vApp is deleted.

Managing Organization Virtual Data Center Networks

4

Organization VDC networks are created and assigned to your organization VDC 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 backed by either NSX Data Center for vSphere.

You can use direct, routed, internal, and imported organization virtual data center networks backed by NSX-T Data Center.

Table 4-1. Types of Organization VDC Networks

Data Center Type Network	Description
Direct	An organization VDC network with a direct connection to one of the external networks that are provisioned by the **system administrator** and are backed by vSphere resources. Direct networks are only supported for organization VDCs that are backed by NSX Data Center for vSphere. Accessible by multiple organization VDCs. Virtual machines belonging to different organization VDCs can connect to and see traffic on this network. This network provides direct layer 2 connectivity to virtual machines outside of the organization VDC. Virtual machines outside of this organization VDC can connect to virtual machines in the organization VDC directly. **Note** Only your **system administrator** can add a direct organization VDC network. Can be IPv4 or IPv6.
Isolated (Internal)	Accessible only by the same organization VDC. Only virtual machines in this organization VDC can connect to and see traffic on the internal organization VDC network. Isolated networks are supported for organization VDCs backed by NSX-T Data Center and for organization VDC NSX Data Center for vSphere. The isolated organization VDC network provides an organization VDC 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 VDC. Machines outside of the organization VDC have no connectivity to machines in the organization VDC.
Routed	Accessible only by the same organization VDC. Only virtual machines in this organization VDC can connect to this network. This network also provides controlled access to an external network. As a **system administrator** or an **organization administrator**, you 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.

Table 4-1. Types of Organization VDC Networks (continued)

Data Center Type Network	Description
Imported	This network uses an existing NSX-T logical switch. Only a **system administrator** can import a network.
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. Cross-VDC networking requires NSX Data Center for vSphere. Can be IPv4 only. For information about cross-VDC networks, see Chapter 5 Managing Cross-Virtual Data Center Networking.

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

This chapter includes the following topics:

View the Available Organization VDC Networks

You can view the available organization virtual data center networks.

Prerequisites

This operation requires the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.

Procedure

- 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.

You see a list of the available networks that you can sort by name.

What to do next

You can add a new network. You can also edit, delete or reset an existing network.

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. For example, you can isolate a network that contains sensitive information and have a separate network that is associated with an edge gateway and connected to the Internet.

You can create an isolated VDC network that is backed by a network pool. Your service provider can also create an isolated VDC network that is backed by an NSX-T logical switch.

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 **Add**.
3. On the **Select Network Type** page, select **Isolated** and click **Next**.
4. Enter a meaningful name for your organization VDC network.
5. Enter the Classless Inter-Domain Routing (CIDR) settings for the isolated network.

   Use the format *network_gateway_IP_address*/*subnet_prefix_length*, for example, `192.167.1.1/24`.
6. (Optional) Enter a description of the organization VDC network.

7 (Optional) To make the organization VDC network available to other organization VDCs within the same organization, toggle on the **Shared** option.

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.

8 Click **Next**.

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

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

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

c (Optional) To modify or remove IP addresses and ranges, click **Modify** or **Remove**.

10 Click **Next**.

11 (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.

12 Click **Next**.

13 On the **Ready to Complete** page, review the organization VDC network settings that you have provided, and click **Finish**.

Add a Routed Organization Virtual Data Center Network

To control the access to an external network, you can add a routed organization VDC 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.

You can add a mix of routed and isolated organization VDC networks to meet the needs of your organization. For example, you can add a network that is associated with an edge gateway and connected to the Internet, while having an isolated network that contains sensitive information.

You can add an IPv4 or IPv6 routed 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 **Add**.
3. On the **Select Network Type** page, select **Routed** and click **Next**.
4. Enter a meaningful name for your organization VDC network.
5. Enter the Classless Inter-Domain Routing (CIDR) settings for the routed organization VDC network.

   Use the format *network_gateway_IP_address*/*subnet_prefix_length*, for example, `192.167.1.1/24`.
6. (Optional) Enter a description of the organization VDC network.
7. (Optional) To make the organization VDC network available to other organization VDCs within the same organization, toggle on the **Shared** option.

   One potential use case is when an application within an Organization VDC 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 share the same network pool.
8. Click **Next**.
9. On the **Edge Connection** page, select an edge gateway with which to associate the organization VDC network.

   If the organization VDC includes more than one edge gateway, you must select an edge gateway for this network to connect to. To support another routed network, the Edge Gateway must show a value of at least 1 in the # Available Networks column.
10. From the **Interface Type** drop-down menu, select the interface type.

Option	Description
Internal	Connects to one of the Edge gateway's internal interfaces. The maximum number of networks that are allowed is 9.
Distributed	Creates the network on a distributed logical router connected to this edge gateway. The maximum number of networks that are allowed is 400.
Subinterface	Extends an organization VDC network. vCloud Director identifies the network to use to extend through L2 VPN. vCloud Director, with the help of NSX network virtualization, creates a trunk interface type for this network. The maximum number of networks that are allowed is 200.

11 (Optional) To enable tagging of guest VLANs on this network, toggle on the **Guest VLAN Allowed** option.

12 Click **Next**.

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

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

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

   c (Optional) To modify or remove IP addresses and ranges, click **Modify** or **Remove**.

14 Click **Next**.

15 (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.

16 Click **Next**.

17 On the **Ready to Complete** page, review the organization VDC network settings that you have provided, and click **Finish**.

Add a Direct Organization Virtual Data Center Network

To connect to an external network by a direct route, **System administrators** can set up a direct connection.

If you log in to the vCloud Director Tenant Portal as an **organization administrator** and attempt to create a direct organization virtual data center network, you receive a warning message that you have insufficient rights.

Prerequisites

This operation is restricted to system administrators.

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 **Add**.

3 On the **Select Network Type** page, select **Direct** and click **Next**.

4 Enter a meaningful name for your organization VDC network.

5 (Optional) Enter a description of the organization VDC network.

6 (Optional) To make the organization VDC network available to other organization VDCs within the same organization, toggle on the **Shared** option.

7 On the **External Network Connection** page, select the external network to which you want your new organization virtual data center network to connect directly, and click **Next**.

8 On the **Ready to Complete** page, review the organization VDC network settings that you have provided, and click **Finish**.

Add an Organization VDC Network with an Imported NSX-T Logical Switch

System administrators can create an organization VDC network by importing a logical switch from an associated NSX-T Manager instance.

Note With an NSX-T logical switch, you can create only an IPv4 isolated organization network. You cannot create a direct organization network based on an NSX-T logical switch.

Prerequisites

- This operation is restricted to **system administrators**.
- The provider virtual data center that backs the target organization virtual data center must be associated with an NSX-T Manager instance.
- The **system administrator** must create at least one NSX-T logical switch that is not in use by other organization virtual data center networks.

For information about creating and configuring NSX-T logical switches, see the *NSX-T Administration Guide*.

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 **Add**.

3 On the **Select Network Type** page, select **Import** and click **Next**.

4 Enter a name and, optionally, a description for the new organization VDC network, and click **Next**.

5 From the list of available NSX-T logical switches, select the target switch by clicking the radio button next to the switch name, and click **Next**.

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

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

   If the switch is configured with a subnet, this information is prepopulated.

7 (Optional) Configure the DNS settings and the static IP pool.

   You can add multiple IP addresses and IP ranges.

8 Click **Next**.

9 Review the **Ready to Complete** page and click **Finish**.

Edit the General Settings of an Organization Virtual Data Center Network

You can modify the properties of organization VDC networks.

Prerequisites

These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes 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 the name of the organization VDC network that you want to view or edit.

3 On the **General** tab, click **Edit**.

   a Edit the name and the description of the network.

   b Toggle on or off the **Shared** option to share or to not share the organization VDC network with other virtual data centers within the same organization.

4 Click **Save**.

Convert an Organization Virtual Data Center Network

After you create an organization VDC network, you can convert the network from isolated to routed, and the reverse.

Prerequisites

These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes 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 the name of the organization VDC network that you want to convert.

3 On the **General** tab, click **Edit**.

4 Click **Connection**.

5 To connect to an edge gateway or to isolate the network from all other networks, toggle on the **Connect to an edge gateway** option or toggle the same option off.

Option	Action
Convert an isolated network to a routed network.	1 Toggle on the **Connect to an edge gateway** option. 2 Select the edge gateway to connect to from the list of available edge gateways. 3 Select the interface type. 4 To allow a guest VLAN, toggle the **Guest VLAN Allowed** option.
Convert a routed network to an isolated network.	Toggle off the **Connect to an edge gateway** option.

6 Click **Save**.

You converted the organization VDC network.

Convert the Interface of a Routed Organization VDC Network

You can change the interface of a network from internal to subinterface or distributed routing, for example, by editing the network properties.

Note Cross-VDC networks cannot be converted.

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 the name of the network that you want to convert.

3 Click the name of the organization VDC network that you want to edit.

4 On the **General** tab, click **Edit**.

5 Click **Connection**.

6 From the **Interface Type** drop-down menu, select the interface type.

Option	Description
Internal	Connects to one of the Edge gateway's internal interfaces. The maximum number of networks that are allowed is 9.
Distributed	Creates the network on a distributed logical router connected to this edge gateway. The maximum number of networks that are allowed is 400.
Subinterface	Extends an organization VDC network. vCloud Director identifies the network to use to extend through L2 VPN. vCloud Director, with the help of NSX network virtualization, creates a trunk interface type for this network. The maximum number of networks that are allowed is 200.

7 Click **Save**.

View the IP Addresses Used for an Organization Virtual Data Center Network

You can view a list of the IP addresses from an organization virtual data center network IP pool that are currently in use.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated or routed organization virtual data center network.

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 the name of the network for which you want to see the used IP addresses.

3 Click the **IP Management** tab.

4 Click **IP Allocations** to see which IP addresses are currently in use.

Add IP Addresses to an Organization Virtual Data Center Network IP Pool

If an organization virtual data center network is running out of IP addresses, you can add more addresses to its IP pool.

You cannot add IP addresses to external organization virtual data center networks that have a direct connection.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated or routed organization virtual data center network.

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 the name of the network that you want to edit.
3. Click the **IP Management** tab.

   The **Static IP Pools** option is selected by default.
4. Click the **Edit** button on the right.

   In the **Edit network** window, you see the gateway CIDR and the IP address ranges, if any.
5. In the **Static IP Pools** text box, enter the IP address or range of IP addresses and click **Add**.

   Note For cross-VDC networks, the IP addresses must not overlap with the IP addresses that are assigned to the other organization VDC networks from the same stretched network.
6. Click **Save**.

The IP address or range of IP addresses are added to the network IP pool.

Edit or Remove IP Ranges Used in an Organization Virtual Data Center Network

If an organization virtual data center network contains IP addresses that you no longer need, you can edit the addresses or delete them from the IP pool.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated or routed organization virtual data center network.

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 the name of the network that you want to edit.
3. Click the **IP Management** tab.

   The **Static IP Pools** option is selected by default.

4 Click the **Edit** button on the right.
   - To modify an IP range, select the range, make the necessary edits, and click **Modify**.
   - To remove an IP range, select the range, and click **Remove**.
5 Click **Save**.

Edit the DNS Settings of an Organization Virtual Data Center Network

You can edit the DNS settings of an organization virtual data center network.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated or routed organization virtual data center network.

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 the name of the network that you want to edit.
3 Click the **IP Management** tab.
4 Select **DNS** and click the **Edit** button on the right.
5 Edit the primary DNS, the secondary DNS, and the DNS suffix information as necessary.
6 Click **Save**.

Configure DHCP Settings for an Isolated Organization Virtual Data Center Network

You can edit the DHCP settings of an isolated organization VDC network. The DHCP service of an organization VDC network provides IP addresses from its address pool to VM NICs that are configured to request an address from DHCP. The service provides the address when the virtual machine powers on.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated organization virtual data center network.

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 the name of the network that you want to edit.

3 Click the **IP Management** tab.

4 Select **DHCP**.

The DHCP settings display on the right.

5 To enable DHCP, click **Edit** on the right of **DHCP Pools Service**.

6 Toggle on the **DHCP Pools Service** and click **Save**.

Addresses requested by DHCP clients are pulled from a DHCP pool.

7 Create a DHCP pool for the network.

a Click **Add**.

b Enter an IP address range for the pool.

The IP address range that you specify cannot overlap with the static IP address pool for the organization virtual data center.

c Specify the default lease time for the DHCP addresses in seconds.

The default value is 3,600 seconds.

d Specify the maximum lease time for the DHCP addresses in seconds.

This is the maximum length of time that the DHCP-assigned IP addresses are leased to the virtual machines. The default value is 7,200 seconds.

8 Click **Save**.

Edit or Delete an Existing DHCP Pool for a Network

If you no longer need a DHCP pool within your isolated organization virtual data center network, you can either delete the pool, or edit it.

Prerequisites

- These operations require the predefined **organization administrator** or **system administrator** roles or a role that includes an equivalent set of rights.
- Verify that your network is an isolated organization virtual data center network.

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 the name of the network that you want to edit.

3 Click the **IP Management** tab.

4 Select **DHCP**.

The DHCP settings display on the right.

5 Edit or delete an existing DHCP pool.

Option	Action
Edit a DHCP pool.	1 Select the DHCP pool that you want to edit. 2 Click the **Edit** button. 3 Update the IP address range for the pool. 4 Edit the default lease time for the DHCP addresses in seconds. 5 Edit the maximum lease time for the DHCP addresses in seconds. 6 Click **Save**.
Delete a DHCP pool.	1 Select the DHCP pool that you want to delete. 2 Click the **Delete** button.

Reset an Organization Virtual Data Center Network

If the network services, such as DHCP settings or firewall settings which are associated with an organization virtual data center network are not working as expected, you can reset the network.

When you reset the organization virtual data center network, you force the network DHCP service gateway to be redeployed. This operation results in a temporary disruption of the DHCP services and no network services are available while the network is resetting.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- The network is not connected to any virtual machines, vApps, or other networks.

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. Select an organization VDC network.
3. Click **Reset** and confirm the reset operation.

Delete an Organization Virtual Data Center Network

If you no longer need an organization virtual data center network, you can delete the network.

Prerequisites

- This operation requires the rights included in the predefined **Organization Administrator** role or an equivalent set of rights.
- The network is not connected to virtual machines, vApps, or other networks.

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 the radio button next to the name of the target network and click **Delete**.
3. To confirm, click **OK**.

Managing Cross-Virtual Data Center Networking

5

To create a network across multiple organization virtual data centers, you first group the virtual data centers, then create a stretched network in the data center group. A data center group can have either a common egress point configuration or an egress point configuration for each network fault domain.

Cross-virtual data center networking requires NSX Data Center for vSphere.

Data center group

A group of up to four virtual data centers that are configured to share multiple egress points. A data center group can have one of the following egress points configurations:

Egress Points Configuration Type	Description
Common egress points configuration	The data center group can be configured with one active egress point and one standby egress point. The two egress points are common to all participating virtual data centers across all network fault domains in the data center group.
Egress points configuration per fault domain	The data center group can be configured with one active egress point for each network fault domain in the data center group. Standby egresses cannot be created.

An organization can have multiple data center groups. An organization virtual data center can participate in multiple data center groups.

The participating organization virtual data centers can belong to different vCloud Director sites. See Configure and Manage Multisite Deployments.

Network Fault Domain

The network provider scope, typically representing the underlying vCenter Server instance with the associated NSX Manager.

Egress point	An edge gateway that connects a data center group or network fault domain to the Internet. The edge gateway must belong to a virtual data center from the data center group. BGP routes are configured on the edge gateway representing the egress point and the universal router of the virtual data center group or network fault domain. Existing routes on the edge gateway are not affected.
Stretched network	A layer 2 network that is stretched across all virtual data centers in a data center group. Can be IPv4 only.

This chapter includes the following topics:

Managing Data Center Groups

After you create a data center group, you can edit the network topology of a data center group. You can add and remove virtual data centers from the group. You can swap, replace, and remove egress points. You can fix configuration failures by performing different synchronization tasks.

You cannot convert a common egress configuration to an egress configuration per fault domain or the reverse.

Create and Configure a Data Center Group with a Common Egress Configuration

You can create and configure a virtual data center group with a common egress configuration, where you set a pair of edge gateways that act as an active and stand-by egress points for all participating virtual data centers.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- Your **system administrator** must enable the target virtual data centers for cross-virtual data center networking.

Procedure

1 Create a Data Center Group with a Common Egress Configuration

   You can group between two and four virtual data centers in a data center group with a common egress configuration.

2 Add an Active Egress Point

   To connect your data center group to the Internet, you must add an active egress point to its network topology.

Create a Data Center Group with a Common Egress Configuration

You can group between two and four virtual data centers in a data center group with a common egress configuration.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 Click **New datacenter group**.

3 Enter a name and, optionally, a description for the new data center group.

4 Select **Common Egress Points** and click **Next**.

5 On the **Datacenters** page, select at least two and up to four data centers for the new data center group, and click **Next**.

The **Datacenters** page contains a list of the virtual data centers that are enabled for cross-virtual data center networking by the **system administrator**.

6 Review the data center group details, and click **Finish**.

The newly created virtual data center group is listed in the **Datacenter Groups** view.

Add an Active Egress Point

To connect your data center group to the Internet, you must add an active egress point to its network topology.

Prerequisites

The **system administrator** created at least one edge gateway on any of the virtual data centers that are participating in the data center group.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 Click **Add egress point**.

   The **Add Active Egress Point** page that opens provides a list of the edge gateways which belong to the participating virtual data centers.

4 Select the edge gateway that you want to act as an active egress point for this data center group, and click **Add**.

BGP routes are configured on the edge gateway representing the egress point and the universal router of the virtual data center group. Existing routes on the edge gateway are not affected.

The diagram of the network topology is updated with the newly added egress point. The traffic from the participating virtual data centers to the Internet is represented with a solid blue line.

Add a Standby Egress Point

In virtual data center groups with common egress configurations, you can add a secondary egress point, which acts as a standby egress point for fault tolerance scenarios.

Prerequisites

Apart from the edge gateway that acts as an active egress point, you must have at least one more edge gateway in any of the virtual data centers that are participating in the group.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 Click **Add stand-by egress point**.

   The **Add Stand-by Egress Point** page opens providing a list of the unused edge gateways that belong to the participating virtual data centers. The edge gateway that is in use by the active egress point in this virtual datacenter group is not displayed.

4 Select the edge gateway that you want to act as a stand-by egress point for this data center group, and click **Add**.

BGP routes are configured on the edge gateway representing the egress point and the universal router of the virtual data center group. Existing routes on the edge gateway are not affected.

The diagram of the network topology is updated with the newly added egress point. The traffic from the participating virtual data centers to the Internet in fault tolerance scenarios is represented with a dashed blue line.

Create and Configure a Data Center Group with a Fault Domain Egress Configuration

You can create and configure a virtual data center group with a fault domain egress configuration, where you configure an edge gateway that acts as an active egress points for each network fault domain in the group. Standby egresses cannot be created in a datacenter group with a fault domain egress configuration.

Prerequisites

This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.

Procedure

1 Create a Data Center Group with a Fault Domain Egress Configuration

   You can group between two and four virtual data centers in a data center group with a fault domain egress configuration.

2 Add an Egress Point for a Fault Domain

   To connect the virtual data centers from a network fault domain in a data center group to the Internet, you must add an egress point to this network fault domain. You can add an egress point to each network fault domain in the data center group. Stand-by egress points are not supported in a data center group with a fault domain egress configuration.

Create a Data Center Group with a Fault Domain Egress Configuration

You can group between two and four virtual data centers in a data center group with a fault domain egress configuration.

Prerequisites

The **system administrator** enabled the target virtual data centers for cross-virtual data center networking.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.

2 Click **New datacenter group**.

3 Enter a name and, optionally, a description for the new data center group.

4 Select **Egress Points per Fault Domain** and click **Next**.

5 On the **Datacenters** page, select at least two and up to four data centers for the new data center group, and click **Next**.

   The **Datacenters** page contains a list of the virtual data centers that are enabled for cross-virtual data center networking by the **system administrator**.

6 Review the data center group details, and click **Finish**.

The newly created virtual data center group is listed in the **Datacenter Groups** view.

Add an Egress Point for a Fault Domain

To connect the virtual data centers from a network fault domain in a data center group to the Internet, you must add an egress point to this network fault domain. You can add an egress point to each network fault domain in the data center group. Stand-by egress points are not supported in a data center group with a fault domain egress configuration.

Prerequisites

Apart from the edge gateways that are in use as egress points in this data center group, you must have at least one unused edge gateway in any of the participating virtual data centers.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 On the diagram of the network topology, click the target network fault domain.

Network fault domains are represented with solid lines and their names at the bottom of the diagram.

The selected fault domain is marked in blue.

4 Click **Add egress point**.

The **Add Active Egress Point** page opens providing a list of the edge gateways that belong to the participating virtual data centers.

5 Select the edge gateway that you want to act as an egress point for this fault domain, and click **Add**.

BGP routes are configured on the edge gateway representing the egress point and the universal router of the network fault domain. Existing routes on the edge gateway are not affected.

The diagram of the network topology is updated with the newly added egress point. The traffic from the virtual data centers in the network fault domain to the Internet is represented with a continuous blue line.

View a Data Center Group

You can view the data center groups in your organization and details about their current configuration.

Prerequisites

This operation requires the **System Administrator** role or a role with the **VDC Group: View VDC Group** right published to the organization.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

Add a Virtual Data Center to a Data Center Group

You can add a virtual data center to a data center group, as a result stretching the existing networks to the new virtual data center.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- The data center group contains less than four virtual data centers.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 Click **Add datacenter**.

4 On the **Datacenters** page, select the data center that you want to add to the data center group and click **Finish**.

The **Datacenters** page contains a list virtual data centers that are enabled for cross-virtual data center networking by the system administrator.

Note A data center group must contain up to four virtual data centers.

Remove a Virtual Data Center from a Data Center Group

You can remove a virtual data center from a data center group, as a result unstretching the existing networks from this virtual data center.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- The data center group must contain at least three virtual data centers.
- The virtual data center that you want to remove must not provide an egress point to the data center group.

Procedure

1. From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.
2. In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.
3. In the upper right corner of the card of the target virtual data center, click the three dots, and click **Remove**.
4. To confirm, click **Remove**.

The virtual data center is removed from the network topology diagram of the data center group.

Synchronize a Data Center Group

To reapply the data center group network configurations and ensure that all participating virtual data centers are active, you can synchronize the data center group.

Note During the data center group synchronization process, the data center group becomes unavailable for a few seconds, because the universal router synchronizes in NSX.

Prerequisites

This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.

Procedure

1. From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.
2. In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 Click **Sync datacenter group**.

4 To confirm, click **OK**.

Swap the Egress Points in a Data Center Group With a Common Egress Configuration

After you configure an active and stand-by egress points in a data center group with a common egress configuration, you can swap the roles of the egress points. The active egress point can become a stand-by egress point and the reverse.

Prerequisites

This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 Click **Swap egress points**.

4 To confirm, click **OK**.

The diagram of the network topology is updated with the new traffic routes. The traffic to the Internet is now redirected to the new active egress point.

Replace the Edge Gateway of an Egress Point

You can replace the edge gateway that represents an active or standby egress point in a data center group.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- The new edge gateway must not be in use by other egress points in the data center group.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 If you are replacing an egress point from a network fault domain configuration, on the network topology diagram, select the network fault domain of the target egress point.

Network fault domains are represented with solid lines and domain names at the bottom of the diagram.

The selected network fault domain is marked in blue.

4 In the upper right corner of the card of the target egress point, click the three dots, and click **Replace**.

The **Replace Egress Point** page opens providing a list of the edge gateways that belong to the participating virtual data centers.

5 Select the new edge gateway and click **Replace**.

BGP routes are removed from the old edge gateway and configured on the new edge gateway representing the egress point and the universal router of the virtual data center group.

The network topology diagram is updated with the name of the new edge gateway.

Remove an Egress Point

To disconnect a data center group or network fault domain from the Internet, you can remove its egress point.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- If you want to remove an active egress point that is paired with a stand-by egress point, you must swap the egress points or remove the stand-by egress point.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 If you are removing an egress point from a network fault domain configuration, on the network topology diagram, select the network fault domain of the target egress point.

   Network fault domains are represented with solid lines and domain names at the bottom of the diagram.

   The selected network fault domain is marked in blue.

4 In the upper right corner of the card of the target egress point, click the three dots, and click **Delete**.

5 To confirm, click **OK**.

BGP routes are removed from the edge gateway representing the egress point if it is not in use by other universal routers.

The egress point is removed from the network topology diagram.

Synchronize Routes and Egress Points

You can reapply the dynamic routing configuration to a data center group or network fault domain and its associated egress points by synchronizing the routes. You can ensure that an egress point is properly connected to the data center group by synchronizing the egress point.

Prerequisites

- This operation requires the **System Administrator** role or a role with the **VDC Group: Configure VDC Group** right published to the organization.
- You configured an egress point for the target data center group or network fault domain.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 If you are synchronizing a network fault domain in a data center group, on the network topology diagram, select the target network fault domain.

   Network fault domains are represented with solid lines and domain names at the bottom of the diagram.

   The selected network fault domain is marked in blue.

4 To reapply the dynamic routing configuration to the group or network fault domain and its associated egress points, click **Sync routes**, and click **OK**.

5 To synchronize an egress point with its data center group, in the upper right corner of the card of the target egress point, click the three dots, click **Sync**, and click **OK**.

Managing Stretched Networks

After you create and configure a data center group, you can create and manage stretched layer 2 networks spanning the participating virtual data centers.

At a virtual data center level, stretched networks appear as organization virtual data center networks of cross-VDC routing type.

Add a Stretched Network

You can create a stretched network across all virtual data centers that are participating in a data center group.

You can add only an IPv4 stretched network.

Prerequisites

This operation requires the predefined **Organization Administrator** role or a role with the **Organization VDC Network: Edit Properties** right.

Procedure

1. From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.

2. In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3. In the left panel, click **Stretched Networks**.

   The list of stretched networks displays in a grid view.

4. Click **Add**.

5. Enter a name and, optionally, a description for the new stretched network.

6. Enter the network Classless Inter-Domain Routing (CIDR) settings, and click **Create**.

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

You can see the newly created network in the list of stretched network for the data center group.

An organization virtual data center network of cross-VDC routing type is created for each participating virtual data center. You can see the newly created networks in the **Datacenters** view of the participating virtual data centers by clicking **Networks**. If a virtual machine or vApp connects to such an organization virtual data center network, this virtual machine or vApp connects to the stretched network.

What to do next

For each corresponding cross-VDC organization virtual data center network, you can assign static IP addresses and IP pools. See Add IP Addresses to an Organization Virtual Data Center Network IP Pool.

For DNS and DHCP configurations for virtual machines attached to a stretched network, you can use the vCloud OpenAPI. To examine the vCloud OpenAPI documentation, go to `https://vCloud_Director_IP_address_or_host_name/docs`. To view code samples and test vCloud OpenAPI calls, go to `https://vCloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name`.

View or Edit a Stretched Network

You can view the name, the description, and the CIDR settings of a stretched network. You can edit only the name and description of a stretched network.

For information about editing the static IP pool allocation for a stretched network at a virtual data center level, see Add IP Addresses to an Organization Virtual Data Center Network IP Pool.

Prerequisites

- Viewing stretched networks requires the predefined **Organization Administrator** role or a role with the **Organization VDC Network: View Properties** right.
- Editing stretched networks requires the predefined **Organization Administrator** role or a role with the **Organization VDC Network: Edit Properties** right.

Procedure

1. From the main menu (☰), select **Datacenter Groups**.

   The list of data center groups displays in a card view.
2. In the card of the target data center group, click **Details**.

   You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.
3. In the left panel, click **Stretched Networks**.

   The list of stretched networks displays in a grid view.
4. Click the radio button next to the name of the target network, and click **Edit**.
5. Edit the network details and click **Save**.

Delete a Stretched Network

You can remove stretched network that you no longer use.

Prerequisites

- This operation requires the predefined **Organization Administrator** role or a role with the **Organization VDC Network: Edit Properties** right.
- The corresponding organization virtual data center networks must not be connected to any virtual machines or vApps.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 In the left panel, click **Stretched Networks**.

The list of stretched networks displays in a grid view.

4 Click the radio button next to the name of the target network, and click **Delete**.

5 To confirm, click **Delete**.

The corresponding organization virtual data center networks are removed from all participating virtual data centers.

Synchronize a Stretched Network

To ensure that all participating virtual data centers can access their stretched network, you can synchronize the stretched network.

Prerequisites

This operation requires the predefined **Organization Administrator** role or a role with the **Organization VDC Network: Edit Properties** right.

Procedure

1 From the main menu (☰), select **Datacenter Groups**.

The list of data center groups displays in a card view.

2 In the card of the target data center group, click **Details**.

You are redirected to the **Network Topology** view for this data center group. You can see a diagram of the current network topology, which depicts the participating virtual data centers with their network fault domains, the egress points if configured, and the traffic routes.

3 In the left panel, click **Stretched Networks**.

The list of stretched networks displays in a grid view.

4 Click the radio button next to the name of the target network, and click **Sync**.

5 To confirm, click **OK**.

Advanced Networking Capabilities for vCloud Director Tenants

6

vCloud Director provides the advanced networking capabilities powered by the NSX network virtualization software that offer enhanced security controls and routing and network scaling capabilities in a cloud environment.

Using these networking capabilities, you can achieve unprecedented security and isolation in your organization virtual data center. These capabilities deliver the following benefits:

- Dynamic routing. The NSX capabilities in your vCloud Director environment support routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) to simplify network integration between systems, to provide redundancy and continuity in a cloud-hosted application deployment.
- Fine-grained network security and isolation. The NSX capabilities in your vCloud Director environment support the use of object-based rule definitions to provide stateful network traffic isolation without requiring multiple virtual networks. This zero-trust security model prevents intruders from gaining full network access if an application or virtual machine is compromised. Network configuration is simplified by using the same network security policies to protect applications wherever they are physically located in the vCloud Director environment and to extend your zero-trust security model for portable security no matter where an application is deployed.
- Additional capabilities provided by NSX are enhanced VPN support for point-to-site (IPsec VPN) and user (SSL VPN-Plus) connectivity, enhanced load balancing for HTTPS, and expanded network scalability.

You can configure two types of firewalls: the edge gateway firewall and the distributed firewall. For more information about the differences between these firewalls, see Firewall Configuration Using the Tenant Portal.

You access these advanced networking capabilities using the vCloud Director tenant portal or the vCloud Director Service Provider Admin Portal. The edge gateway must first be converted to an advanced edge gateway. See Convert an Edge Gateway to an Advanced Edge Gateway.

Important IPv6 edge gateways support limited services. IPv6 edge gateways support edge firewalls, distribute firewalls, and static routing.

This chapter includes the following topics:

Getting Started with vCloud Director Advanced Networking

You use the vCloud Director Advanced Networking to perform management tasks on an organization in a vCloud Director system. You can manage distributed firewalls and other advanced networking capabilities that are provided by the VMware NSX® software components made available to an organization by a vCloud Director system administrator.

The typical users of Advanced Networking are:

- vCloud Director **system administrators**, who might use the tenant portal to configure the distributed firewall and other advanced networking capabilities for an organization.
- **Organization administrators**, who use the tenant portal to manage the distributed firewall and other advanced networking capabilities that the **system administrator** has made available to that organization.

Firewall Configuration Using the Tenant Portal

Using the tenant portal, you can configure the firewall capabilities provided by the NSX software in your vCloud Director organization virtual data center. You can create firewall rules for distributed firewalls to provide security between virtual machines in an organization virtual data center and firewall rules to apply to an edge gateway firewall to protect the virtual machines in an organization virtual data center from outside network traffic.

Note The tenant portal provides the ability to configure both edge gateway firewalls and distributed firewalls.

The NSX logical firewall technology consists of two components to address different deployment use cases. The edge gateway firewall focuses on North-South traffic enforcement while the distributed firewall focuses on East-West access controls.

Key Differences Between Edge Gateway Firewalls and Distributed Firewalls

An edge gateway firewall monitors North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality.

A distributed firewall provides the capability to isolate and secure each virtual machine and application down to the layer 2 (L2) level. Configuring distributed firewalls effectively quarantines any external or internal network security compromise, isolating East-West traffic between virtual machines on the same network segment. Security policies are centrally managed, inheritable, and nestable, so networking and security administrators can manage them at scale. Additionally, once deployed, defined security policies follow the virtual machines or applications when they move between different virtual data centers.

About Firewall Rules

As described in the NSX product documentation, in NSX, the firewall rules defined on the centralized level are referred to as pre rules. You can also add rules at an individual edge gateway level, and those rules are referred to as local rules.

Each traffic session is checked against the top rule in the firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. Rules are displayed in the following order:

1 User-defined pre rules have the highest priority, and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.

2 Auto-plumbed rules (rules that enable control traffic to flow for edge gateway services).

3 Local rules defined at an edge gateway level.

4 Default distributed firewall rule

For more information about how the NSX software enforces firewall rules, see *Change the Order of a Firewall Rule* in the *NSX Administration* documentation.

Edge Gateway Firewall

The firewall for the edge gateway helps you meet key perimeter security requirements, such as building DMZs based on IP/VLAN constructs, tenant-to-tenant isolation in multi-tenant virtual data centers, Network Address Translation (NAT), partner (extranet) VPNs, and user-based SSL VPNs.

The edge gateway firewall capability in the vCloud Director environment is provided by the NSX software. In NSX, this firewall capability is also referred to as the edge firewall. The edge gateway firewall monitors North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality.

For more detailed information about the capabilities provided by the edge gateway firewall of the NSX software, see the *NSX Administration* documentation.

Managing an NSX Data Center for vSphere Edge Gateway Firewall

To protect traffic to and from an edge gateway, you can create and manage firewall rules on that edge gateway.

For information about protecting traffic traveling between virtual machines in an organization virtual data center, see Managing Distributed Firewall Rules Using the Tenant Portal.

Rules created on the distributed firewall screen that have an advanced edge gateway specified in their Applied To column are not displayed in the Firewall screen for that advanced edge gateway .

The edge gateway firewall rules for an edge gateway are displayed in the **Firewall** screen and are enforced in the following order:

1. Internal rules, also known as auto-plumbed rules. These internal rules enable control traffic to flow for edge gateway services.
2. User-defined rules.
3. Default rule.

The default rule settings apply to traffic that does not match any of the user-defined firewall rules. The default rule is displayed at the bottom of the rules on the Firewall screen.

In the tenant portal, use the **Enable** toggle on the Firewall Rules screen of the edge gateway to disable or enable an edge gateway firewall.

Convert an Edge Gateway to an Advanced Edge Gateway

To work with an edge gateway in the tenant portal, you need to convert it to an advanced edge gateway. Once you convert it to an advanced edge gateway, you can use the tenant portal to configure the static and dynamic routing capabilities that are provided by the NSX software for those advanced edge gateways.

Prerequisites

You have an existing edge gateway.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore, and select **Edges** from the left panel.
2. Select the edge gateway to edit.
3. Click **Convert to Advanced**.

Your edge gateway is converted to an advanced edge gateway.

What to do next

Once you have converted to an advanced edge gateway, you can configure settings by selecting the gateway and clicking **Services**.

Add an NSX Data Center for vSphere Edge Gateway Firewall Rule

You use the edge gateway **Firewall** tab to add firewall rules for that edge gateway. You can add multiple NSX Edge interfaces and multiple IP address groups as the source and destination for these firewall rules.

Specifying **internal** for a source or a destination of a rule indicates traffic for all subnets on the port groups connected to the NSX edge gateway. If you select **internal** as the source, the rule is automatically updated when additional internal interfaces are configured on the NSX gateway.

Note Edge gateway firewall rules on internal interfaces do not work when the edge gateway is configured for dynamic routing.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. If the **Firewall Rules** screen is not already visible, click the **Firewall** tab.
3. To add a rule below an existing rule in the firewall rules table, click in the existing row and then click the **Create** button.

   A row for the new rule is added below the selected rule, and is assigned any destination, any service, and the **Allow** action by default. When the system-defined default rule is the only rule in the firewall table, the new rule is added above the default rule.
4. Click in the **Name** cell and type in a name.

5 Click in the **Source** cell and use the now visible icons to select a source to add to the rule:

Option	Description
Click the IP icon	Type the source value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The edge gateway firewall supports both IPv4 and IPv6 formats.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the **Select objects** window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the **Select objects** window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the **Select objects** window

6 Click in the **Destination** cell and perform one of the following options:

Option	Description
Click the IP icon	Type the destination value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The edge gateway firewall supports both IPv4 and IPv6 formats.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the **Select objects** window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the **Select objects** window

7 Click in the **Service** cell of the new rule and click the **+** icon to specify the service as a port-protocol combination:

a Select the service protocol.

b Type the port numbers for the source and destination ports, or specify **any**.

c Click **Keep**.

8 In the **Action** cell of the new rule, configure the action for the rule.

Option	Description
Accept	Allows traffic from or to the specified sources, destinations, and services.
Deny	Blocks traffic from or to the specified sources, destinations, and services.

9 Click **Save changes**.

The save operation can take a minute to complete.

Modify NSX Data Center for vSphere Edge Gateway Firewall Rules

You can edit and delete only the user-defined firewall rules that were added to an edge gateway. You cannot edit or delete an auto-generated rule or a default rule, except for changing the action setting of the default rule. You can change the priority order of user-defined rules.

For details about the available settings for the various cells of a rule, see Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Click the **Firewall** tab.

3 Manage the firewall rules.

- Disable a rule by clicking the green check mark in its **No.** cell. The green check mark turns to a red disabled icon. If the rule is disabled and you want to enable the rule, click the red disabled icon.
- Edit a rule name by double-clicking in its **Name** cell and typing the new name.
- Modify the settings for a rule, such as the source or action settings, by selecting the appropriate cell and using the displayed controls.
- Delete a rule by selecting it and clicking the **Delete** button located above the rules table.
- Hide system-generated rules by using the **Show only user-defined rules** toggle.
- Move a rule up or down in the rules table by selecting the rule and clicking the up and down arrow buttons located above the rules table.

4 Click **Save changes**.

Distributed Firewall

The distributed firewall allows you to segment organization virtual datacenter entities, such as virtual machines, based on virtual machine names and attributes.

The distributed firewall capability in the vCloud Director environment is provided by the NSX software. As described in the *NSX Administration* documentation, this distributed firewall is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on objects like virtual machine names and on network constructs like

IP addresses or IP set addresses. Firewall rules are enforced at the vNIC level of each virtual machine to provide consistent access control even when the virtual machine is moved to a new ESXi host by vSphere vMotion. This distributed firewall supports a micro-segmentation security model where East-West traffic can be inspected at near line rate processing.

As described in the *NSX Administration* documentation,, for layer 2 (L2) packets, the distributed firewall creates a cache for performance boost. Layer 3 (L3) packets are processed in the following sequence:

1 All packets are checked for an existing state.

2 When a state match is found, the packets are processed.

3 When a state match is not found, the packets are processed through the rules until a match is found.

- For TCP packets, a state is set only for packets with a SYN flag. However, rules that do not specify a protocol (service ANY), can match TCP packets with any combination of flags.
- For UDP packets, 5-tuple details are extracted from the packet. When a state does not exist in the state table, a new state is created using the extracted 5-tuple details. Subsequently received packets are matched against the state that was just created.
- For ICMP packets, ICMP type, code, and packet direction are used to create a state.

The distributed firewall can help in creating identity-based rules as well. Administrators can enforce access control based on the user's group membership as defined in the enterprise Active Directory (AD). Some use cases for when you might use identity-based firewall rules are:

- Users accessing virtual applications using a laptop or mobile device where AD is used for user authentication
- Users accessing virtual applications using VDI infrastructure where the virtual machines are Microsoft Windows based

For more detailed information about the capabilities provided by the NSX software's distributed firewall, see the *NSX Administration* documentation.

Enable the Distributed Firewall on an Organization Virtual Data Center using the Tenant Portal

Before you can use the tenant portal to work with the distributed firewall capabilities on an organization virtual data center, the distributed firewall must be enabled for that organization virtual data center. A vCloud Director system administrator or a user granted the ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE right can enable the distributed firewall on an organization virtual data center.

You use the Distributed Firewall screen in the tenant portal to enable the distributed firewall for an organization virtual data center.

Prerequisites

Verify that the organization to which the organization virtual data center belongs has the following rights assigned to it:

- Organization vDC Distributed Firewall: Enable/Disable
- Organization vDC Distributed Firewall: Configure Rules
- Organization vDC Distributed Firewall: View Rules

The vCloud Director system administrator assigns rights to an organization. The Organization vDC Distributed Firewall: Enable/Disable right is required for enabling the distributed firewall using the user interface in the tenant portal. The Organization vDC Distributed Firewall: View Rules right is required for viewing the firewall rules in the tenant portal and the Organization vDC Distributed Firewall: Configure Rules right is required for configuring the firewall rules using the tenant portal.

Verify that you have an assigned role that grants you the right named Organization vDC Distributed Firewall: Enable/Disable. Of the pre-defined roles in a vCloud Director system, only the System Administrator role has that right by default.

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 the organization virtual data center for which you want to configure distributed firewall rules.
3. Click **Configure Services**.
4. Enable distributed firewall on the **Distributed Firewall** tab.

What to do next

For a description of the default distributed firewall rule, see Managing Distributed Firewall Rules Using the Tenant Portal.

Managing Distributed Firewall Rules Using the Tenant Portal

As described in the *NSX Administration Guide*, default firewall settings apply to traffic that does not match any of the user-defined firewall rules. In the vCloud Director Tenant Portal, the default distributed firewall rule is labeled Default Allow Rule.

The distributed firewall capability must be enabled on an organization virtual data center before you can manage the distributed firewall settings using the vCloud Director Tenant Portal.

The default distributed firewall rule is configured to allow all layer 3 and layer 2 traffic to pass through the organization virtual data center. This setting is indicated by the Allow set in the Action column in the user interface. The default rule is always at the bottom of the rules table.

Important You cannot delete or modify the default distributed firewall rules.

Add a Distributed Firewall Rule

You first add a distributed firewall rule to the scope of the organization virtual data center. Then you can narrow down the scope at which you want to apply the rule. The distributed firewall allows you to add multiple objects at the source and destination levels for each rule, which helps reduce the total number of firewall rules to be added.

For information about the predefined services and service groups that you can use in a rule, see View Services Available for Firewall Rules and View Service Groups Available for Firewall Rules.

Prerequisites

- Enable the Distributed Firewall on an Organization Virtual Data Center using the Tenant Portal
- If you want to use an IP set as a source or destination in a rule, Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration.
- If you want to use an MAC set as a source or destination in a rule, Create a MAC Set for Use in Firewall Rules.
- If you want to use a Security group as a source or destination in a rule, Create 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 the security services VDC network for which you want to modify firewall rules, and click **Configure Services**.

   The Security Services screen displays.
3. Select the type of rule you want to create. You have the option to create a general rule or an Ethernet rule.

   Layer 3 (L3) rules are configured on the **General** tab. Layer 2 (L2) rules are configured on the **Ethernet** tab.
4. To add a rule below an existing rule in the firewall table, click in the existing row and then click the **Create** () button.

   A row for the new rule is added below the selected rule, and is assigned any destination, any service, and the **Allow** action by default . When the system-defined Default Allow rule is the only rule in the firewall table, the new rule is added above the default rule.
5. Click in the **Name** cell and type in a name.

6 Click in the **Source** cell and use the now visible icons to select a source to add to the rule:

Action	Description
Click the IP icon	Applicable for rules defined on the **General** tab. Type the source value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The distributed firewall supports IPv4 format only.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the **Select objects** window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the **Select objects** window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the **Select objects** window

7 Click in the **Destination** cell and perform one of the following actions:

Action	Description
Click the IP icon	Applicable for rules defined on the **General** tab. Type the destination value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The distributed firewall supports IPv4 format only.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the **Select objects** window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the **Select objects** window

8 Click in the **Service** cell of the new rule and perform one of the following actions:

Action	Description
Click the IP icon	To specify the service as a port–protocol combination: a Select the service protocol. b Type the port numbers for the source and destination ports, or specify **any**, and click **Keep**.
Click the + icon	To select a pre-defined service or service group, or define a new one: a Select one or more objects and add them to the filter. b Click **Keep**.

9 In the **Action** cell of the new rule, configure the action for the rule.

Option	Description
Allow	Allows traffic from or to the specified sources, destinations, and services.
Deny	Blocks traffic from or to the specified sources, destinations, and services.

10 In the **Direction** cell of the new rule, select whether the rule applies to incoming traffic, outgoing traffic, or both.

11 If this is a rule on the **General** tab, in the **Packet Type** cell of the new rule, select a packet type of **Any**, **IPV4**, or **IPV6**.

12 Select the **Applied To** cell, and use the **+** icon to define the object scope to which this rule is applicable.

When the rule contains virtual machines in the **Source** and **Destination** cells, you must add both the source and destination virtual machines to the rule's **Applied To** for the rule to work correctly.

Important IP address groups (IP sets), MAC address groups (MAC sets), and security groups containing either IP sets or MAC sets are not valid input parameters.

13 Click **Save Changes**.

Edit a Distributed Firewall Rule

In a vCloud Director environment, to modify an existing distributed firewall rule of an organization virtual data center, use the **Distributed Firewall** screen.

For details about the available settings for the various cells of a rule, see Add a Distributed Firewall Rule.

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 the security services VDC network for which you want to modify firewall rules, and click **Configure Services**.

The Security Services screen displays.

3 Perform any of the following actions to manage the distributed firewall rules:

- Disable a rule by clicking the green check mark in its **No.** cell.

  The green check mark turns to a red disabled icon. If the rule is disabled and you want to enable the rule, click the red disabled icon.

- Edit a rule name by double-clicking in its **Name** cell and typing the new name.
- Modify the settings for a rule, such as the source or action settings, by selecting the appropriate cell and using the displayed controls.

- Delete a rule by selecting it and clicking the **Delete** () button located above the rules table.
- Move a rule up or down in the rules table by selecting the rule and clicking the up and down arrow buttons located above the rules table.

4 Click **Save Changes**.

Managing Edge Gateway DHCP

You configure your edge gateways to provide Dynamic Host Configuration Protocol (DHCP) services to virtual machines connected to the associated organization virtual data center networks.

As described in the NSX documentation, an NSX edge gateway capabilities include IP address pooling, one-to-one static IP address allocation, and external DNS server configuration. Static IP address binding is based on the managed object ID and interface ID of the requesting client virtual machine.

The DHCP service for an NSX edge gateway:

- Listens on the internal interface of the edge gateway for DHCP discovery.
- Uses the IP address of the internal interface of the edge gateway as the default gateway address for all clients.
- Uses the broadcast and subnet mask values of the internal interface for the container network.

In the following situations, you need to restart the DHCP service on the client virtual machines that have the DHCP-assigned IP addresses:

- You changed or deleted a DHCP pool, default gateway, or DNS server.
- You changed the internal IP address of the edge gateway instance.

Note If the DNS settings on a DHCP-enabled edge gateway are changed, the edge gateway might stop providing DHCP services. If this situation occurs, use the **DHCP Service Status** toggle on the DHCP Pools screen to disable and then reenable DHCP on that edge gateway. See Add a DHCP IP Pool.

Add a DHCP IP Pool

You can configure the IP pools needed for a DHCP service of an NSX Data Center for vSphere edge gateway. DHCP automates IP address assignment to virtual machines connected to organization virtual data center networks.

As described in the *NSX Administration* documentation, the DHCP service requires a pool of IP addresses. An IP pool is a sequential range of IP addresses within the network. Virtual machines protected by the edge gateway that do not have an address binding are allocated an IP address from this pool. IP pool ranges cannot intersect one another, thus one IP address can belong to only one IP pool.

Note At least one DHCP IP pool must be configured to have the DHCP service status turned on.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **DHCP > Pools** .

3 If DHCP service is not currently enabled, turn on the **DHCP Service Status** toggle.

> **Note** Add at least one DHCP IP pool before saving changes after turning on the **DHCP Service Status** toggle. If no DHCP IP pools are listed on the screen and you turn on the **DHCP Service Status** toggle and save the changes, the screen displays with the toggle turned off.

4 Under DHCP Pools, click the **Create** () button, specify the details for the DHCP pool, and click **Keep**.

Option	Description
IP Range	Type in a range of IP addresses.
Domain Name	Domain name of the DNS server.
Auto Configure DNS	Turn on this toggle to use the DNS service configuration for this IP pool DNS binding. If enabled, the **Primary Name Server** and **Secondary Name Server** are set to **Auto**.
Primary Name Server	When you do not enable **Auto Configure DNS**, type your primary DNS server IP address of your primary DNS server. This IP address is used for hostname-to-IP address resolution.
Secondary Name Server	When you do not enable **Auto Configure DNS**, type your secondary DNS server IP address. This IP address is used for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. When you do not specify the default gateway IP address, the internal interface of the edge gateway instance is taken as the default gateway.
Subnet Mask	Type the subnet mask of the edge gateway interface.
Lease Never Expires	Enable this toggle to keep the IP addresses that are assigned out of this pool bound to their assigned virtual machines forever. When you select this option, **Lease Time** is set to infinite.
Lease Time (Seconds)	Length of time (in seconds) that the DHCP-assigned IP addresses are leased to the clients. The default lease time is one day (86400 seconds). **Note** You cannot specify a lease time when you select **Lease never expires**.

5 Click **Save changes**.

vCloud Director updates the edge gateway to provide DHCP services.

Add DHCP Bindings

If you have services running on a virtual machine and do not want the IP address to be changed, you can bind the virtual machine MAC address to the IP address. The IP address you bind must not overlap a DHCP IP pool.

Prerequisites

You have the MAC addresses for the virtual machines for which you want to set up bindings.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 On the **DHCP > Bindings** tab, click the **Create** () button, specify the details for the binding, and click **Keep**.

Option	Description
MAC Address	Type the MAC address of the virtual machine that you want bound to the IP address.
Host Name	Type the host name you want set for that virtual machine when the virtual machine requests a DHCP lease.
IP Address	Type the IP address you want bound to the MAC address.
Subnet Mask	Type the subnet mask of the edge gateway interface.
Domain Name	Type the domain name of the DNS server.
Auto Configure DNS	Enable this toggle to use the DNS service configuration for this DNS binding. If enabled, the **Primary Name Server** and **Secondary Name Server** are set to **Auto**.
Primary Name Server	When you do not select **Auto Configure DNS**, type your primary DNS server IP address of your primary DNS server. This IP address is used for hostname-to-IP address resolution.
Secondary Name Server	When you do not select **Auto Configure DNS**, type your secondary DNS server IP address. This IP address is used for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. When you do not specify the default gateway IP address, the internal interface of the edge gateway instance is taken as the default gateway.

Option	Description
Lease Never Expires	Enable this toggle to keep the IP address bound to that MAC address forever. When you select this option, **Lease Time** is set to infinite.
Lease Time (Seconds)	Length of time (in seconds) that the DHCP-assigned IP addresses are leased to the clients. The default lease time is one day (86400 seconds). **Note** You cannot specify a lease time when you select **Lease never expires**.

3 Click **Save changes**.

Configuring DHCP Relay for NSX Data Center for vSphere Edge Gateways

The DHCP relay capability provided by NSX in your vCloud Director environment enables you to leverage your existing DHCP infrastructure from within your vCloud Director environment without any interruption to the IP address management in your existing DHCP infrastructure. DHCP messages are relayed from virtual machines to the designated DHCP servers in your physical DHCP infrastructure, which allows IP addresses controlled by the NSX software to continue to be synchronized with IP addresses in the rest of your DHCP-controlled environments.

The DHCP relay configuration of an edge gateway can list several DHCP servers. Requests are sent to all listed servers. While relaying the DHCP request from the VMs, the edge gateway adds a gateway IP address to the request. The external DHCP server uses this gateway address to match a pool and allocate an IP address for the request. The gateway address must belong to a subnet of the edge gateway interface.

You can specify a different DHCP server for each edge gateway and can configure multiple DHCP servers on each edge gateway to provide support for multiple IP domains.

Note

- DHCP relay does not support overlapping IP address spaces.
- DHCP relay and DHCP service cannot run on the same vNIC at the same time. If a relay agent is configured on a vNIC, a DHCP pool cannot be configured on the subnets of that vNIC. See the *NSX Administration Guide* for details.

Specify a DHCP Relay Configuration for an NSX Data Center for vSphere Edge Gateway

The NSX software in your vCloud Director environment provides the capability for the edge gateway to relay DHCP messages to DHCP servers external to your vCloud Director organization virtual data center. You can configure the DHCP relay capability of the edge gateway.

As described in the *NSX Administration* documentation, the DHCP servers can be specified using an existing IP set, IP address block, domain, or a combination of all of these. DHCP messages are relayed to every specified DHCP server.

You must also configure at least one DHCP relay agent. A DHCP relay agent is an interface on the edge gateway from which the DHCP requests are relayed to the external DHCP servers.

Prerequisites

If you want to use an IP set to specify a DHCP server, verify that an IP set exists as a grouping object available to the edge gateway. See Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. Navigate to **DHCP > Relay**.
3. Use the on-screen fields to specify the DHCP servers by IP addresses, domain names, or IP sets.

   You select from existing IP sets using **Add** () button to browse the available IP sets.
4. Configure a DHCP relay agent and add its configuration to the on-screen table by clicking the **Add** () button, selecting a vNIC and its gateway IP address, and then clicking **Keep**.

   By default, the Gateway IP Address matches the primary address of the selected vNIC. You can keep the default or select an alternate address if one is available on that vNIC.
5. Click **Save changes**.

Managing Network Address Translation Using the Tenant Portal

The NSX software in your vCloud Director environment enables the edge gateways to provide a network address translation (NAT) service. Using this capability reduces the number of public IP addresses that an organization must use, for economy and security purposes.

The edge gateway NAT service provides the ability to assign a public address to a virtual machine or group of virtual machines in a private network. To enable your edge gateways to provide access to services running on privately addressed virtual machines in your organization virtual data center, you must configure NAT rules on the edge gateways. In the most common case, you associate a NAT service with an uplink interface on an edge gateway in your vCloud Director environment so that addresses on organization virtual data center networks are not exposed on the external network.

The NAT service configuration is separated into source NAT (SNAT) and destination NAT (DNAT) rules. When you configure a SNAT or a DNAT rule on an edge gateway in the vCloud Director environment, you always configure the rule from the perspective of your organization virtual data center. Specifically, that means you configure the rules in the following ways:

- SNAT: the traffic is traveling from a virtual machine on an internal network in your organization virtual data center (the source) through the Internet to the external network (the destination). A SNAT rule translates the source IP address of the outgoing packets of an organization virtual data center network that are being sent to an external network or to another organization virtual data center network.
- DNAT: the traffic is traveling from the Internet (the source) to a virtual machine inside your organization virtual data center (the destination). A DNAT rule translates the IP address, and optionally the port, of packets received by an organization virtual data center network that are coming from an external network or from another organization virtual data center network.

You can configure NAT rules to create a private IP address space inside your organization virtual data center. This configuration provides the ability to port a private IP address space from one organization virtual data center to another. Configuring NAT rules allows you to use the same private IP addresses for your virtual machines in one organization virtual data center that were used in another.

The NAT rule capability in your vCloud Director environment supports:

- Creating subnets within the private IP address space
- Creating multiple private IP address spaces for an edge gateway
- Configuring multiple NAT rules on multiple edge gateway interfaces

Important You must configure both firewall and NAT rules on an edge gateway for the virtual machines on an edge gateway network to be accessible. By default, edge gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the edge gateway networks. Also, NAT is disabled by default on the edge gateways so that edge gateways are unable to translate the IP addresses of the incoming and outgoing traffic unless you configure NAT on the edge gateways. Attempting to ping a virtual machine on a network after configuring a NAT rule will fail unless you add a firewall rule to allow the corresponding traffic.

Add a SNAT or a DNAT Rule

You can create a source NAT (SNAT) rule to change the source IP address from a public to private IP address or the reverse. You can create a destination NAT (DNAT) rule to change the destination IP address from a public to private IP address or the reverse.

When creating NAT rules, you can specify the original and translated IP addresses by using the following formats:

- IP address; for example, 192.0.2.0
- IP address range; for example, 192.0.2.0-192.0.2.24
- IP address/subnet mask; for example, 192.0.2.0/24

- any

When you configure a SNAT or a DNAT rule on an edge gateway in the vCloud Director environment, you always configure the rule from the perspective of your organization virtual data center. A SNAT rule translates the source IP address of packets sent from an organization virtual data center network out to an external network or to another organization virtual data center network. A DNAT rule translates the IP address, and optionally the port, of packets received by an organization virtual data center network that are coming from an external network or from another organization virtual data center network.

Prerequisites

The public IP addresses must have been added to the NSX Data Center for vSphere edge gateway interface on which you want to add the rule. For DNAT rules, the original (public) IP address must have been added to the edge gateway interface and for SNAT rules, the translated (public) IP address must have been added to the interface.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. Click the **NAT** to view the NAT Rules screen.
3. Depending on which type of NAT rule you are creating, click **DNAT Rule** or **SNAT Rule**.
4. Configure a Destination NAT rule (outside coming inside).

Option	Description
Applied On	Select the interface on which to apply the rule.
Original IP/Range	Type the required IP address. This address must be the public IP address of the edge gateway for which you are configuring the DNAT rule. In the packet being inspected, this IP address or range would be those that appear as the destination IP address of the packet. These packet destination addresses are the ones translated by this DNAT rule.
Protocol	Select the protocol to which the rule applies. To apply this rule on all protocols, select **Any**.
Original Port	(Optional) Select the port or port range that the incoming traffic uses on the edge gateway to connect to the internal network on which the virtual machines are connected. This selection is not available when the **Protocol** is set to **ICMP** or **Any**.
ICMP Type	When you select **ICMP** (an error reporting and a diagnostic utility used between devices to communicate error information) for **Protocol**, select the **ICMP Type** from the drop-down menu. ICMP messages are identified by the type field. By default, the ICMP type is set to any.

Option	Description
Translated IP/Range	Type the IP address or a range of IP addresses to which destination addresses on inbound packets will be translated. These addresses are the IP addresses of the one or more virtual machines for which you are configuring DNAT so that they can receive traffic from the external network.
Translated Port	(Optional) Select the port or port range that inbound traffic is connecting to on the virtual machines on the internal network. These ports are the ones into which the DNAT rule is translating for the packets inbound to the virtual machines.
Description	(Optional) Type a description that helps identify what this rule is doing.
Enabled	Toggle on to enable this rule.
Enable logging	Toggle on to have the address translation performed by this rule logged.

5 Configure a Source NAT rule (inside going outside).

Option	Description
Applied On	Select the interface on which to apply the rule.
Original Source IP/Range	Type the original IP address or range of IP addresses to apply to this rule. These addresses are the IP addresses of one or more virtual machines for which you are configuring the SNAT rule so that they can send traffic to the external network.
Translated Source IP/Range	Type the required IP address. This address is always the public IP address of the gateway for which you are configuring the SNAT rule. Specifies the IP address to which source addresses (the virtual machines) on outbound packets are translated to when they send traffic to the external network.
Description	(Optional) Type a description that helps identify what this rule is doing.
Enabled	Toggle on to enable this rule.
Enable logging	Toggle on to have the address translation performed by this rule logged.

6 Click **Keep** to add the rule to the on-screen table.

7 Repeat the steps to configure additional rules.

8 Click **Save changes** to save the rules to the system.

What to do next

Add corresponding edge gateway firewall rules for the SNAT or DNAT rules you just configured. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Advanced Routing Configuration

You can configure the static and dynamic routing capabilities that are provided by the NSX software for your edge gateways.

To enable dynamic routing, you configure an advanced edge gateway using the Border Gateway Protocol (BGP) or the Open Shortest Path First (OSPF) protocol.

For detailed information about the routing capabilities that NSX provides, see *Routing* in the *NSX Administration* documentation.

You can specify static and dynamic routing for each advanced edge gateway. The dynamic routing capability provides the necessary forwarding information between Layer 2 broadcast domains, which allows you to decrease Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to the locations of the workloads for East-West routing. This capability allows more direct virtual machine to virtual machine communication without the added cost or time needed to extend hops.

Specify Default Routing Configurations for the NSX Data Center for vSphere Edge Gateway

You can specify the default settings for static routing and dynamic routing for an edge gateway.

Note To remove all configured routing settings, use the **CLEAR GLOBAL CONFIGURATION** button at the bottom of the **Routing Configuration** screen. This action deletes all routing settings currently specified on the subscreens: default routing settings, static routes, OSPF, BGP, and route redistribution.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Routing > Routing Configuration**.

3 To enable Equal Cost Multipath (ECMP) routing for this edge gateway, turn on the **ECMP** toggle.

   As described in the *NSX Administration* documentation, ECMP is a routing strategy that allows next-hop packet forwarding to a single destination to occur over multiple best paths. NSX determines these best paths either statically, using configured static routes, or as a result of metric calculations by dynamic routing protocols like OSPF or BGP. You can specify the multiple paths for static routes by specifying multiple next hops on the Static Routes screen.

   For more details about ECMP and NSX, see the routing topics in the *NSX Troubleshooting Guide*.

4 Specify settings for the default routing gateway.

   a Use the **Applied On** drop-down list to select an interface from which the next hop towards the destination network can be reached.

      To see details about the selected interface, click the blue information icon.

   b Type the gateway IP address.

   c Type the MTU.

d (Optional) Type an optional description.

e Click **Save changes**.

5 Specify default dynamic routing settings.

Note If you have IPsec VPN configured in your environment, you should not use dynamic routing.

a Select a router ID.

You can select a router ID in the list or use the **+** icon to enter a new one. This router ID is the first uplink IP address of the edge gateway that pushes routes to the kernel for dynamic routing.

b Configure logging by turning on the **Enable Logging** toggle and selecting the log level.

c Click **OK**.

6 Click **Save changes**.

What to do next

Add static routes. See Add a Static Route.

Configure route redistribution. See Configure Route Redistributions.

Configure dynamic routing. See the following topics:

- Configure BGP
- Configure OSPF

Add a Static Route

You can add a static route for a destination subnet or host.

If ECMP is enabled in the default routing configuration, you can specify multiple next hops in the static routes. See Specify Default Routing Configurations for the NSX Data Center for vSphere Edge Gateway for steps on enabling ECMP.

Prerequisites

As described in the NSX documentation, the next hop IP address of the static route must exist in a subnet associated with one of the NSX Data Center for vSphere edge gateway interfaces. Otherwise, configuration of that static route fails.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Routing > Static Routes**.

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

4 Configure the following options for the static route:

Option	Description
Network	Type the network in CIDR notation.
Next Hop	Type the IP address of the next hop. The next hop IP address must exist in a subnet associated with one of the edge gateway interfaces. If ECMP is enabled, you can type multiple next hops.
MTU	Edit the maximum transmission value for data packets. The MTU value cannot be higher than the MTU value set on the selected edge gateway interface. You can see the MTU set on the edge gateway interface by default on the Routing Configuration screen.
Interface	Optionally, select the edge gateway interface on which you want to add a static route. By default, the interface is selected that matches the next hop address.
Description	Optionally, type a description for the static route.

5 Click **Save changes**.

What to do next

Configure a NAT rule for the static route. See Add a SNAT or a DNAT Rule.

Add a firewall rule to allow traffic to traverse the static route. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Configure OSPF

You can configure the Open Shortest Path First (OSPF) routing protocol for the dynamic routing capabilities of an NSX Data Center for vSphere edge gateway. A common application of OSPF on an edge gateway in a vCloud Director environment is to exchange routing information between edge gateways in vCloud Director.

The NSX edge gateway supports OSPF, an interior gateway protocol that routes IP packets only within a single routing domain. As described in the *NSX Administration* documentation, configuring OSPF on an NSX edge gateway enables the edge gateway to learn and advertise routes. The edge gateway uses OSPF to gather link state information from available edge gateways and construct a topology map of the network. The topology determines the routing table presented to the Internet layer, which makes routing decisions based on the destination IP address found in IP packets.

As a result, OSPF routing policies provide a dynamic process of traffic load balancing between routes of equal cost. An OSPF network is divided into routing areas to optimize traffic flow and limit the size of routing tables. An area is a logical collection of OSPF networks, routers, and links that have the same area identification. Areas are identified by an Area ID.

Prerequisites

A Router ID must be configured . Specify Default Routing Configurations for the NSX Data Center for vSphere Edge Gateway.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Routing > OSPF**.

3 If OSPF is not currently enabled, use the **OSPF Enabled** toggle to enable it.

4 Configure the OSPF settings according to the needs of your organization.

Option	Description
Enable Graceful Restart	Specifies that packet forwarding is to remain uninterrupted when OSPF services are restarted.
Enable Default Originate	Allows the edge gateway to advertise itself as a default gateway to its OSPF peers.

5 (Optional) You can either click **Save changes** or continue with configuring area definitions and interface mappings.

6 Add an OSPF area definition by clicking the **Add** () button, specifying details for the mapping in the dialog box, and clicking **Keep**.

Note By default, the system configures a not-so-stubby area (NSSA) with area ID of 51, and this area is automatically displayed in the area definitions table on the OSPF screen. You can modify or delete the NSSA area.

Option	Description
Area ID	Type an area ID in the form of an IP address or decimal number.
Area Type	Select **Normal** or **NSSA**. NSSAs prevent the flooding of AS-external link-state advertisements (LSAs) into NSSAs. They rely on default routing to external destinations. As a result, NSSAs must be placed at the edge of an OSPF routing domain. NSSA can import external routes into the OSPF routing domain, by that means providing transit service to small routing domains that are not part of the OSPF routing domain.
Area Authentication	Select the type of authentication for OSPF to perform at the area level. All edge gateways within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiver and transmitter must have the same MD5 key. Choices are: ■ **None** No authentication is required. ■ **Password** With this choice, the password you specify in the **Area Authentication Value** field is included in the transmitted packet. ■ **MD5** With this choice, the authentication uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet. Type the Md5 key into the **Area Authentication Value** field.

7 Click **Save changes**, so that the newly configured area definitions are available for selection when you add interface mappings.

8 Add an interface mapping by clicking the **Add** () button, specifying details for the mapping in the dialog box, and clicking **Keep**.

These mappings map the edge gateway interfaces to the areas.

a In the dialog box, select the interface you want to map to an area definition.

The interface specifies the external network that both edge gateways are connected to.

b Select the area ID for the area to map to the selected interface.

c (Optional) Change the OSPF settings from the default values to customize them for this interface mapping.

When configuring a new mapping, the default values for these settings are displayed. In most cases, it is recommended to retain the default settings. If you do change the settings, make sure that the OSPF peers use the same settings.

Option	Description
Hello Interval	Interval (in seconds) between hello packets that are sent on the interface.
Dead Interval	Interval (in seconds) during which at least one hello packet must be received from a neighbor before that neighbor is declared down.
Priority	Priority of the interface. The interface with the highest priority is the designated edge gateway router.
Cost	Overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. The larger the bandwidth, the smaller the cost.

d Click **Keep**.

9 Click **Save changes** in the OSPF screen.

What to do next

Configure OSPF on the other edge gateways that you want to exchange routing information with.

Add a firewall rule that allows traffic between the OSPF-enabled edge gateways. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Make sure that the route redistribution and firewall configuration allow the correct routes to be advertised. See Configure Route Redistributions.

Configure BGP

You can configure Border Gateway Protocol (BGP) for the dynamic routing capabilities of an NSX Data Center for vSphere edge gateway.

As described in the *NSX Administration Guide*, BGP makes core routing decisions by using a table of IP networks or prefixes, which designate network reachability among multiple autonomous systems. In the networking field, the term BGP speaker refers to a networking device that is running BGP. Two BGP speakers establish a connection before any routing information is exchanged. The term BGP neighbor refers to a BGP speaker that has established such a connection. After establishing the connection, the devices exchange routes and synchronize their tables. Each device sends keep alive messages to keep this relationship alive.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Routing > BGP**.

3 If BGP is not currently enabled, use the **Enable BGP** toggle to enable it.

4 Configure the BGP settings according to the needs of your organization.

Option	Description
Enable Graceful Restart	Specifies that packet forwarding is to remain uninterrupted when BGP services are restarted.
Enable Default Originate	Allows the edge gateway to advertise itself as a default gateway to its BGP neighbors.
Local AS	Required. Specify the autonomous system (AS) ID number to use for the local AS feature of the protocol. The value you specify must be a globally unique number between 1 and 65534. The local AS is a feature of BGP. The system assigns the local AS number to the edge gateway you are configuring. The edge gateway advertises this ID when the edge gateway peers with its BGP neighbors in other autonomous systems. The path of autonomous systems that a route would traverse is used as one metric in the dynamic routing algorithm when selecting the best path to a destination.

5 You can either click **Save changes**, or continue to configure settings for the BGP routing neighbors.

6 Add a BGP neighbor configuration by clicking the **Add** () button, specifying details for the neighbor in the dialog box, and clicking **Keep**.

Option	Description
IP Address	Type the IP address of a BGP neighbor for this edge gateway.
Remote AS	Type a globally unique number between 1-65534 for the autonomous system to which this BGP neighbor belongs. This remote AS number is used in the BGP neighbor's entry in the system's BGP neighbors table.
Weight	The default weight for the neighbor connection. Adjust as appropriate for your organization's needs.
Keep Alive Time	The frequency with which the software sends keep alive messages to its peer. The default frequency is 60 seconds. Adjust as appropriate for the needs of your organization.
Hold Down Time	The interval for which the software declares a peer dead after not receiving a keep alive message. This interval must be three times the keep alive interval. The default interval is 180 seconds. Adjust as appropriate for the needs of your organization. Once peering between two BGP neighbors is achieved, the edge gateway starts a hold down timer. Every keep alive message it receives from the neighbor resets the hold down timer to 0. If the edge gateway fails to receive three consecutive keep alive messages, so that the hold down timer reaches three times the keep alive interval, the edge gateway considers the neighbor down and deletes the routes from this neighbor.

Option	Description
Password	If this BGP neighbor requires authentication, type the authentication password. Each segment sent on the connection between the neighbors is verified. MD5 authentication must be configured with the same password on both BGP neighbors, otherwise, the connection between them will not be made.
BGP Filters	Use this table to specify route filtering using a prefix list from this BGP neighbor. **Caution** A `block all` rule is enforced at the end of the filters. Add a filter to the table by clicking the **+** icon and configuring the options. Click **Keep** to save each filter. ■ Select the direction to indicate whether you are filtering traffic to or from the neighbor. ■ Select the action to indicate whether you are allowing or denying traffic. ■ Type the network that you want to filter to or from the neighbor. Type `ANY` or a network in a CIDR format. ■ Type the **IP Prefix GE** and **IP Prefix LE** to use the `le` and `ge` keywords in the IP prefix list.

7 Click **Save changes** to save the configurations to the system.

What to do next

Configure BGP on the other edge gateways that you want to exchange routing information with.

Add a firewall rule that allows traffic to and from the BGP-configured edge gateways. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule for information.

Configure Route Redistributions

By default the router only shares routes with other routers running the same protocol. When you have configured a multi-protocol environment, you must configure route redistribution to have cross-protocol route sharing. You can configure route redistribution for an NSX Data Center for vSphere edge gateway.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Routing > Route Redistribution**.

3 Use the protocol toggles to turn on those protocols for which you want to enable route redistribution.

4 Add IP prefixes to the on-screen table.

   a Click the **Add** () button.

   b Type a name and the IP address of the network in CIDR format.

   c Click **Keep**.

5 Specify redistribution criteria for each IP prefix by clicking the **Add** () button, specifying the criteria in the dialog box, and clicking **Keep**.

Entries in the table are processed sequentially. Use the up and down arrows to adjust the sequence.

Option	Description
Prefix Name	Select a specific IP prefix to apply this criteria to or select **Any** to apply the criteria to all network routes.
Learner Protocol	Select the protocol that is to learn routes from other protocols under this redistribution criteria.
Allow learning from	Select the types of networks from which routes can be learned for the protocol selected in the **Learner Protocol** list.
Action	Select whether to permit or deny redistribution from the selected types of networks.

6 Click **Save changes**.

Load Balancing

The load balancer distributes incoming service requests among multiple servers in such a way that the load distribution is transparent to users. Load balancing helps achieve optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload.

About Load Balancing

The NSX load balancer supports two load balancing engines. The layer 4 load balancer is packet-based and provides fast-path processing. The layer 7 load balancer is socket-based and supports advanced traffic management strategies and DDOS mitigation for back end services.

Load balancing for an edge gateway is configured on the external interface because the edge gateway load balances incoming traffic from the external network. When configuring virtual servers for load balancing, specify one of the available IP addresses you have in your organization VDC.

Load Balancing Strategies and Concepts

A packet-based load balancing strategy is implemented on the TCP and UDP layer. Packet-based load balancing does not stop the connection or buffer the whole request. Instead, after manipulating the packet, it sends it directly to the selected server. TCP and UDP sessions are maintained in the load balancer so that packets for a single session are directed to the same server. You can select Acceleration Enable in both the global configuration and relevant virtual server configuration to enable packet-based load balancing.

A socket-based load balancing strategy is implemented on top of the socket interface. Two connections are established for a single request, a client-facing connection and a server-facing connection. The server-facing connection is established after server selection. For HTTP socket-based implementation, the whole request is received before sending to the selected server with optional L7 manipulation. For HTTPS socket-based implementation, authentication information is exchanged either on the client-facing connection or server-facing connection. Socket-based load balancing is the default mode for TCP, HTTP, and HTTPS virtual servers.

The key concepts of the NSX load balancer are, virtual server, server pool, server pool member, and service monitor.

Virtual Server	Abstract of an application service, represented by a unique combination of IP, port, protocol and application profile such as TCP or UDP.
Server Pool	Group of backend servers.
Server Pool Member	Represents the backend server as member in a pool.
Service Monitor	Defines how to probe the health status of a back end server.
Application Profile	Represents the TCP, UDP, persistence, and certificate configuration for a given application.

Setup Overview

You begin by setting global options for the load balancer. You now create a server pool consisting of back end server members and associate a service monitor with the pool to manage and share the back end servers efficiently.

You then create an application profile to define the common application behavior in a load balancer such as client SSL, server SSL, x-forwarded-for, or persistence. Persistence sends subsequent requests with similar characteristic such as, source IP or cookie are required to be dispatched to the same pool member, without running the load balancing algorithm. The application profile can be reused across virtual servers.

You then create an optional application rule to configure application-specific settings for traffic manipulation such as, matching a certain URL or hostname so that different requests can be handled by different pools. Next, you create a service monitor that is specific to your application or you may use an already existing service monitor if it meets your needs.

Optionally you can create an application rule to support advanced functionality of L7 virtual servers. Some use cases for application rules include content switching, header manipulation, security rules, and DOS protection.

Finally, you create a virtual server that connects your server pool, application profile, and any potential application rules together.

When the virtual server receives a request, the load balancing algorithm considers pool member configuration and runtime status. The algorithm then calculates the appropriate pool to distribute the traffic comprising one or more members. The pool member configuration includes settings such as, weight, maximum connection, and condition status. The runtime status includes current connections, response time, and health check status information. The calculation methods can be round-robin, weighted round-robin, least connection, source IP hash, weighted least connections, URL, URI, or HTTP header.

Each pool is monitored by the associated service monitor. When the load balancer detects a problem with a pool member, it is marked as DOWN. Only UP server is selected when choosing a pool member from the server pool. If the server pool is not configured with a service monitor, all the pool members are considered as UP.

Configure the Load Balancer Service

Global load balancer configuration parameters include overall enablement, selection of the layer 4 or layer 7 engine, and specification of the types of events to log.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Load Balancer** > **Global Configuration**.

3 Select the options you want to enable:

Option	Action
Status	Enable the load balancer by clicking the toggle icon. Enable **Acceleration Enabled** to configure the load balancer to use the faster L4 engine rather than L7 engine. The L4 TCP VIP is processed before the edge gateway firewall so no Allow firewall rule is required. **Note** L7 VIPs for HTTP and HTTPS are processed after the firewall, so when you do not enable acceleration, an edge gateway firewall rule must exist to allow access to the L7 VIP for those protocols. When you enable acceleration, and the server pool is in a non-transparent mode, a SNAT rule is added, so you must ensure that the firewall is enabled on the edge gateway.
Enable Logging	Enable logging so that the edge gateway load balancer collects traffic logs.
Log Level	Choose the severity of events to be collected in the logs.

4 Click **Save changes**.

   The save operation can take a minute to complete.

What to do next

Configure application profiles for the load balancer. See Create an Application Profile.

Create an Application Profile

An application profile defines the behavior of the load balancer for a particular type of network traffic. After configuring a profile, you associate it with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

When you create a profile for HTTPS traffic, the following HTTPS traffic patterns are allowed:

- Client -> HTTPS -> LB (terminate SSL) -> HTTP -> servers
- Client -> HTTPS -> LB (terminate SSL) -> HTTPS -> servers
- Client -> HTTPS-> LB (SSL passthrough) -> HTTPS -> servers
- Client -> HTTP-> LB -> HTTP -> servers

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. Navigate to **Load Balancer** > **Application Profiles**.
3. Click the **Create** () button.
4. Enter a name for the profile.
5. Configure the application profile.

Option	Description
Type	Select the protocol type used to send requests to the server. The list of required parameters depends on the protocol you select. Parameters that are not applicable to the protocol you selected cannot be entered. All other parameters are required.
Enable SSL Passthrough	Click to enable SSL authentication to be passed through to the virtual server. Otherwise SSL authentication takes place at the destination address.
HTTP Redirect URL	(HTTP and HTTPS) Type the URL to which traffic that arrives at the destination address should be redirected.

Option	Description
Persistence	Specify a persistence mechanism for the profile. Persistence tracks and stores session data, such as the specific pool member that serviced a client request. This ensures that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions. The options are: ■ **Source IP** Source IP persistence tracks sessions based on the source IP address. When a client requests a connection to a virtual server that supports source address affinity persistence, the load balancer checks to see if that client previously connected, and if so, returns the client to the same pool member. ■ **MSRDP** (TCP Only) Microsoft Remote Desktop Protocol persistence (MSRDP) maintains persistent sessions between Windows clients and servers that are running the Microsoft Remote Desktop Protocol (RDP) service. The recommended scenario for enabling MSRDP persistence is to create a load balancing pool that consists of members running a Windows Server guest OS, where all members belong to a Windows cluster and participate in a Windows session directory.
Cookie Name	(HTTP and HTTPS) If you specified **Cookie** as the persistence mechanism, type the cookie name. Cookie persistence uses a cookie to uniquely identify the session the first time a client accesses the site. The load balancer refers to this cookie when connecting subsequent requests in the session, so that they all go to the same virtual server.
Mode	Select the mode by which the cookie should be inserted. The following modes are supported: ■ **Insert** The edge gateway sends a cookie. When the server sends one or more cookies, the client will receive one extra cookie (the server cookies plus the edge gateway cookie). When the server does not send any cookies, the client will receive the edge gateway cookie only. ■ **Prefix** Select this option when your client does not support more than one cookie. **Note** All browsers accept multiple cookies. But you might have a proprietary application using a proprietary client that supports only one cookie. The Web server sends its cookie as usual. The edge gateway injects (as a prefix) its cookie information in the server cookie value. This cookie added information is removed when the edge gateway sends it to the server. ■ **App Session** For this option, the server does not send a cookie; instead, it sends the user session information as a URL. For example, `http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD`, where `jsessionid` is the user session information and is used for the persistence. It is not possible to see the App Session persistence table for troubleshooting.

Option	Description
Expires in (Seconds)	Enter a length of time in seconds that persistence stays in effect. Must be a positive integer in the range 1-86400. **Note** For L7 load balancing using TCP source IP persistence, the persistence entry times out if no new TCP connections are made for a period of time, even if the existing connections are still alive.
Insert X-Forwarded-For HTTP header	(HTTP and HTTPS) Select **Insert X-Forwarded-For HTTP** header for identifying the originating IP address of a client connecting to a Web server through the load balancer.
Enable Pool Side SSL	(HTTPS Only) Select **Enable Pool Side SSL** to define the certificate, CAs, or CRLs used to authenticate the load balancer from the server side in the Pool Certificates tab.

6 (HTTPS only) Configure the certificates to be used with the application profile. If the certificates you need do not exist, you can create them from the **Certificates** tab.

Option	Description
Virtual Server Certificates	Select the certificate, CAs, or CRLs used to decrypt HTTPS traffic.
Pool Certificates	Define the certificate, CAs, or CRLs used to authenticate the load balancer from the server side. **Note** Select **Enable Pool Side SSL** to enable this tab.
Cipher	Select the cipher algorithms (or cipher suite) negotiated during the SSL/TLS handshake.
Client Authentication	Specify whether client authentication is to be ignored or required. **Note** When set to required, the client must provide a certificate after the request or the handshake is canceled.

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

The operation can take a minute to complete.

What to do next

Add service monitors for the load balancer to define health checks for different types of network traffic. See Create a Service Monitor.

Create a Service Monitor

You create a service monitor to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Load Balancer** > **Service Monitoring**.

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

4 Enter a name for the service monitor.

5 (Optional) Configure the following options for the service monitor:

Option	Description
Interval	Enter the interval at which a server is to be monitored using the specified **Method**.
Timeout	Enter the maximum time in seconds within which a response from the server must be received.
Max Retries	Enter the number of times the specified monitoring **Method** must fail sequentially before the server is declared down.
Type	Select the way in which you want to send the health check request to the server—HTTP, HTTPS, TCP, ICMP, or UDP. Depending on the type selected, the remaining options in the **New Service Monitor** dialog are enabled or disabled.
Expected	(HTTP and HTTPS) Enter the string that the monitor expects to match in the status line of the HTTP or HTTPS response (for example, HTTP/1.1).
Method	(HTTP and HTTPS) Select the method to be used to detect server status.
URL	(HTTP and HTTPS) Enter the URL to be used in the server status request. **Note** When you select the POST method, you must specify a value for **Send**.
Send	(HTTP, HTTPS, UDP) Enter the data to be sent.
Receive	(HTTP, HTTPS, and UDP) Enter the string to be matched in the response content. **Note** When **Expected** is not matched, the monitor does not try to match the **Receive** content.

Extension	(ALL) Enter advanced monitor parameters as key=value pairs. For example, warning=10 indicates that when a server does not respond within 10 seconds, its status is set as warning. All extension items should be separated with a carriage return character. For example:
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

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

   The operation can take a minute to complete.

Example: Extensions Supported for Each Protocol

Table 6-1. Extensions for HTTP/HTTPS Protocols

Monitor Extension	Description
no-body	Does not wait for a document body and stops reading after the HTTP/HTTPS header. **Note** An HTTP GET or HTTP POST is still sent; not a HEAD method.
max-age=*SECONDS*	Warns when a document is more than SECONDS old. The number can be in the form 10m for minutes, 10h for hours, or 10d for days.
content-type=*STRING*	Specifies a Content-Type header media type in POST calls.
linespan	Allows regex to span newlines (must precede -r or -R).
regex=*STRING* or ereg=*STRING*	Searches the page for regex STRING.
eregi=*STRING*	Searches the page for case-insensitive regex STRING.
invert-regex	Returns CRITICAL when found and OK when not found.
proxy-authorization=*AUTH_PAIR*	Specifies the username:password on proxy servers with basic authentication.
useragent=*STRING*	Sends the string in the HTTP header as `User Agent`.
header=*STRING*	Sends any other tags in the HTTP header. Use multiple times for additional headers.
onredirect=ok|warning|critical|follow|sticky|stickyport	Indicates how to handle redirected pages. `sticky` is like `follow` but stick to the specified IP address. `stickyport` ensures the port stays the same.
pagesize=*INTEGER:INTEGER*	Specifies the minimum and maximum page sizes required in bytes.
warning=DOUBLE	Specifies the response time in seconds to result in a warning status.
critical=DOUBLE	Specifies the response time in seconds to result in a critical status.

Table 6-2. Extensions for HTTPS Protocol Only

Monitor Extension	Description
sni	Enables SSL/TLS hostname extension support (SNI).
certificate=**INTEGER**	Specifies the minimum number of days a certificate has to be valid. The port defaults to 443. When this option is used, the URL is not checked.
authorization=AUTH_PAIR	Specifies the username:password on sites with basic authentication.

Table 6-3. Extensions for TCP Protocol

Monitor Extension	Description
escape	Allows for the use of `\n`, `\r`, `\t`, or `\` in a send or quit string. Must come before a send or quit option. By default, nothing is added to send and `\r\n` is added to the end of quit.
all	Specifies all expect strings need to occur in a server response. By default, `any` is used.
quit=*STRING*	Sends a string to the server to cleanly close the connection.
refuse=ok|warn|crit	Accepts TCP refusals with states `ok`, `warn`, or `criti`. By default, uses state `crit`.
mismatch=ok|warn|crit	Accepts expected string mismatches with states `ok`, `warn`, or `crit`. By default, uses state `warn`.
jail	Hides output from the TCP socket.
maxbytes=*INTEGER*	Closes the connection when more than the specified number of bytes are received.
delay=*INTEGER*	Waits the specified number of seconds between sending the string and polling for a response.
certificate=*INTEGER*[,*INTEGER*]	Specifies the minimum number of days a certificate has to be valid. The first value is `#days` for warning and the second value is critical (if not specified - 0).
ssl	Uses SSL for the connection.
warning=DOUBLE	Specifies the response time in seconds to result in a warning status.
critical=DOUBLE	Specifies the response time in seconds to result in a critical status.

What to do next

Add server pools for your load balancer. See Add a Server Pool for Load Balancing.

Add a Server Pool for Load Balancing

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Load Balancer** > **Pools**.

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

4 Type a name and, optionally, a description for the load balancer pool.

5 Select a balancing method for the service from the **Algorithm** drop-down menu:

Option	Description
ROUND-ROBIN	Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server processing time remains equally distributed.
IP-HASH	Selects a server based on a hash of the source and destination IP address of each packet.
LEASTCONN	Distributes client requests to multiple servers based on the number of connections already open on the server. New connections are sent to the server with the fewest open connections.
URI	The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This option ensures that a URI is always directed to the same server as long as the server does not go down.
HTTPHEADER	HTTP header name is looked up in each HTTP request. The header name in parenthesis is not case sensitive which is similar to the ACL 'hdr()' function. If the header is absent or does not contain any value, the round robin algorithm is applied. The HTTP HEADER algorithm parameter has one option `headerName=<name>`. For example, you can use **`host`** as the HTTP HEADER algorithm parameter.
URL	URL parameter specified in the argument is looked up in the query string of each HTTP GET request. If the parameter is followed by an equal sign = and a value, then the value is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This process is used to track user identifiers in requests and ensure that a same user ID is always sent to the same server as long as no server goes up or down. If no value or parameter is found, then a round robin algorithm is applied. The URL algorithm parameter has one option `urlParam=<url>`.

6 Add members to the pool.

a Click the **Add** (+) button.

b Enter the name for the pool member.

c Enter the IP address of the pool member.

d Enter the port at which the member is to receive traffic from the load balancer.

e Enter the monitor port at which the member is to receive health monitor requests.

f In the **Weight** text box, type the proportion of traffic this member is to handle. Must be an integer in the range 1-256.

g (Optional) In the **Max Connections** text box, type the maximum number of concurrent connections the member can handle.

When the number of incoming requests exceeds the maximum, requests are queued and the load balancer waits for a connection to be released.

h (Optional) In the **Min Connections** text box, type the minimum number of concurrent connections a member must always accept.

i Click **Keep** to add the new member to the pool.

The operation can take a minute to complete.

7 (Optional) To make client IP addresses visible to the back end servers, select **Transparent**.

When **Transparent** is not selected (the default value), back end servers see the IP address of the traffic source as the internal IP address of the load balancer.

When **Transparent** is selected, the source IP address is the actual IP address of the client and the edge gateway must be set as the default gateway to ensure that return packets go through the edge gateway.

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

The operation can take a minute to complete.

What to do next

Add virtual servers for your load balancer. A virtual server has a public IP address and services all incoming client requests. See Add a Virtual Server.

Add an Application Rule

You can write an application rule to directly manipulate and manage IP application traffic.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Load Balancer** > **Application Rules**.

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

4 Enter the name for the application rule.

5 Enter the script for the application rule.

For information on the application rule syntax, see http://cbonte.github.io/haproxy-dconv/configuration-1.5.html.

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

The operation can take a minute to complete.

What to do next

Associate the new application rule to a virtual server added for the load balancer. See Add a Virtual Server.

Add a Virtual Server

Add an NSX Data Center for vSphere edge gateway internal or uplink interface as a virtual server. A virtual server has a public IP address and services all incoming client requests.

By default, the load balancer closes the server TCP connection after each client request.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **Load Balancer** > **Virtual Servers**.

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

4 On the **General** tab, configure the following options for the virtual server:

Option	Description
Enable Virtual Server	Click to enable the virtual server.
Enable Acceleration	Click to enable acceleration.
Application Profile	Select an application profile to be associated with the virtual server.
Name	Type a name for the virtual server.
Description	Type an optional description for the virtual server.
IP Address	Type or browse to select the IP address that the load balancer listens on.
Protocol	Select the protocol that the virtual server accepts. You must select the same protocol used by the selected **Application Profile**.
Port	Type the port number that the load balancer listens on.
Default Pool	Choose the server pool that the load balancer will use.
Connection Limit	(Optional) Type the maximum concurrent connections that the virtual server can process.
Connection Rate Limit (CPS)	(Optional) Type the maximum incoming new connection requests per second.

5 (Optional) To associate application rules with the virtual server, click the **Advanced** tab and complete the following steps:

   a Click the **Add** () button.

   The application rules created for the load balancer appear. If necessary, add application rules for the load balancer. See Add an Application Rule.

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

   The operation can take a minute to complete.

What to do next

Create an edge gateway firewall rule to permit traffic to the new virtual server (the destination IP address). See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule

Secure Access Using Virtual Private Networks

You can configure the VPN capabilities that are provided by the NSX software for your edge gateways. You can configure VPN connections to your organization virtual data center using an SSL VPN-Plus tunnel, an IPsec VPN tunnel, or an L2 VPN tunnel.

As described in the *NSX Administration Guide*, the NSX edge gateway supports these VPN services:

- SSL VPN-Plus, which allows remote users to access private corporate applications.
- IPsec VPN, which offers site-to-site connectivity between an NSX edge gateway and remote sites which also have NSX or which have third-party hardware routers or VPN gateways.
- L2 VPN, which allows extension of your organization virtual data center by allowing virtual machines to retain network connectivity while retaining the same IP address across geographical boundaries.

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

Note vCloud Director does not support multiple VPN tunnels between the same two edge gateways. If there is an existing tunnel between two edge gateways and you want to add another subnet to the tunnel, delete the existing VPN tunnel and create a new one that includes the new subnet.

After you configure VPN tunnels for an edge gateway, you can use a VPN client from a remote location to connect to the organization virtual data center that is backed by that edge gateway.

Configure SSL VPN-Plus

The SSL VPN-Plus services for an edge gateway in a vCloud Director environment enable remote users to connect securely to the private networks and applications in the organization virtual data centers backed by that edge gateway. You can configure various SSL VPN-Plus services on the edge gateway.

In your vCloud Director environment, the edge gateway SSL VPN-Plus capability supports network access mode. Remote users must install an SSL client to make secure connections and access the networks and applications behind the edge gateway. As part of the edge gateway SSL VPN-Plus configuration, you add the installation packages for the operating system and configure certain parameters. See Add an SSL VPN-Plus Client Installation Package for details.

Configuring SSL VPN-Plus on an edge gateway is a multi-step process.

Prerequisites

Verify that all SSL certificates needed for the SSL VPN-Plus have been added to the **Certificates** screen. See SSL Certificate Management.

Note On an edge gateway, port 443 is the default port for HTTPS. For the SSL VPN functionality, the edge gateway HTTPS port must be accessible from external networks. The SSL VPN client requires the edge gateway IP address and port that are configured in the Server Settings screen on the **SSL VPN-Plus** tab to be reachable from the client system. See Configure SSL VPN Server Settings.

Procedure

1 Navigate to the SSL-VPN Plus Screen

You can navigate to the SSL-VPN Plus screen to begin configuring the SSL-VPN Plus service for an NSX Data Center for vSphere edge gateway.

2 Configure SSL VPN Server Settings

These server settings configure the SSL VPN server, such as the IP address and port the service listens on, the cipher list of the service, and its service certificate. When connecting to the edge gateway, remote users specify the same IP address and port you set in these server settings.

3 Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway

The remote users are assigned virtual IP addresses from the static IP pools that you configure using the **IP Pools** screen on the **SSL VPN-Plus** tab.

4 Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway

Use the Private Networks screen on the **SSL VPN-Plus** tab to configure the private networks. The private networks are the ones you want the VPN clients to have access to, when the remote users connect using their VPN clients and the SSL VPN tunnel. The enabled private networks will be installed in the routing table of the VPN client.

5 Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway

Use the **Authentication** screen on the **SSL VPN-Plus** tab to set up a local authentication server for the edge gateway SSL VPN service and optionally enable client certificate authentication. This authentication server is used to authenticate the connecting users. All users configured in the local authentication server will be authenticated.

6 Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server

Use the **Users** screen on the **SSL VPN-Plus** tab to add accounts for your remote users to the local authentication server for the edge gateway SSL VPN service.

7 Add an SSL VPN-Plus Client Installation Package

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

8 Edit SSL VPN-Plus Client Configuration

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

9 Customize the General SSL VPN-Plus Settings for an Edge Gateway

By default, the system sets some SSL VPN-Plus settings on an edge gateway in your vCloud Director environment. You can use the **General Settings** screen on the **SSL VPN-Plus** tab in the vCloud Director tenant portal to customize these settings.

Navigate to the SSL-VPN Plus Screen

You can navigate to the SSL-VPN Plus screen to begin configuring the SSL-VPN Plus service for an NSX Data Center for vSphere edge gateway.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Click the **SSL VPN-Plus** tab.

What to do next

On the **General** screen, configure the default SSL VPN-Plus settings. See Customize the General SSL VPN-Plus Settings for an Edge Gateway.

Configure SSL VPN Server Settings

These server settings configure the SSL VPN server, such as the IP address and port the service listens on, the cipher list of the service, and its service certificate. When connecting to the edge gateway, remote users specify the same IP address and port you set in these server settings.

If your edge gateway is configured with multiple, overlay IP address networks on its external interface, the IP address you select for the SSL VPN server can be different than the default external interface of the edge gateway.

While configuring the SSL VPN server settings, you must choose which encryption algorithms to use for the SSL VPN tunnel. You can choose one or more ciphers. Carefully choose the ciphers according to the strengths and weaknesses of your selections.

By default, the system uses the default, self-signed certificate that the system generates for each edge gateway as the default server identity certificate for the SSL VPN tunnel. Instead of this default, you can choose to use a digital certificate that you have added to the system on the **Certificates** screen.

Prerequisites

- Verify that you have met the prerequisites described in Configure SSL VPN-Plus.
- If you choose to use a service certificate different than the default one, import the required certificate into the system. See Add a Service Certificate to the Edge Gateway.
- Navigate to the SSL-VPN Plus Screen.

Procedure

1. On the **SSL VPN-Plus** screen, click **Server Settings**.
2. Click **Enabled**.
3. Select an IP address from the drop-down menu.
4. (Optional) Enter a TCP port number.

   The TCP port number is used by the SSL client installation package. By default, the system uses port 443, which is the default port for HTTPS/SSL traffic. Even though a port number is required, you can set any TCP port for communications.

   Note The SSL VPN client requires the IP address and port configured here to be reachable from the client systems of your remote users. If you change the port number from the default, ensure that the IP address and port combination are reachable from the systems of your intended users.
5. Select an encryption method from the cipher list.
6. Configure the service Syslog logging policy.

   Logging is enabled by default. You can change the level of messages to log or disable logging.
7. (Optional) If you want to use a service certificate instead of the default system-generated self-signed certificate, click **Change server certificate**, selection a certificate, and click **OK**.
8. Click **Save changes**.

What to do next

Note The edge gateway IP address and the TCP port number you set must be reachable by your remote users. Add an edge gateway firewall rule that allows access to the SSL VPN-Plus IP address and port configured in this procedure. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Add an IP pool so that remote users are assigned IP addresses when they connect using SSL VPN-Plus. See Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway.

Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway

The remote users are assigned virtual IP addresses from the static IP pools that you configure using the **IP Pools** screen on the **SSL VPN-Plus** tab.

Each IP pool added in this screen results in an IP address subnet configured on the edge gateway. The IP address ranges used in these IP pools must be different from all other networks configured on the edge gateway.

Note SSL VPN assigns IP addresses to the remote users from the IP pools based on the order the IP pools appear in the on-screen table. After you add the IP pools to the on-screen table, you can adjust their positions in the table using the up and down arrows.

Prerequisites

- Navigate to the SSL-VPN Plus Screen.
- Configure SSL VPN Server Settings.

Procedure

1 On the **SSL VPN-Plus** tab, click **IP Pools**.

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

3 Configure the IP pool settings.

Option	Action
IP Range	Enter an IP address range for this IP pool, such as `127.0.0.1–127.0.0.9.`. These IP addresses will be assigned to VPN clients when they authenticate and connect to the SSL VPN tunnel.
Netmask	Enter the netmask of the IP pool, such as `255.255.255.0`.
Gateway	Enter the IP address that you want the edge gateway to create and assign as the gateway address for this IP pool. When the IP pool is created, a virtual adapter is created on the edge gateway virtual machine and this IP address is configured on that virtual interface. This IP address can be any IP within the subnet that is not also in the range in the **IP Range** field.
Description	(Optional) Enter a description for this IP pool.
Status	Select whether to enable or disable this IP pool.
Primary DNS	(Optional) Enter the name of the primary DNS server that will be used for name resolution for these virtual IP addresses.
Secondary DNS	(Optional) Enter the name of the secondary DNS server to use.
DNS Suffix	(Optional) Enter the DNS suffix for the domain the client systems are hosted on, for domain-based host name resolution.
WINS Server	(Optional) Enter the WINS server address for the needs of your organization.

4 Click **Keep**.

The IP pool configuration is added to the on-screen table.

What to do next

Add private networks that you want accessible to your remote users connecting with SSL VPN-Plus. See Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway.

Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway

Use the Private Networks screen on the **SSL VPN-Plus** tab to configure the private networks. The private networks are the ones you want the VPN clients to have access to, when the remote users connect using their VPN clients and the SSL VPN tunnel. The enabled private networks will be installed in the routing table of the VPN client.

The private networks is a list of all reachable IP networks behind the edge gateway that you want to encrypt traffic for a VPN client, or exclude from encrypting. Each private network that requires access through an SSL VPN tunnel must be added as a separate entry. You can use route summarization techniques to limit the number of entries.

- SSL VPN-Plus allows remote users to access private networks based on the top-down order the IP pools appear in the on-screen table. After you add the private networks to the on-screen table, you can adjust their positions in the table using the up and down arrows.
- If you select to enable TCP optimization for a private network, some applications such as FTP in active mode might not work within that subnet. To add an FTP server configured in active mode, you must add another private network for that FTP server and disable TCP optimization for that private network. Also, the private network for that FTP server must be enabled and appear in the on-screen table above the TCP-optimized private network.

Prerequisites

- Navigate to the SSL-VPN Plus Screen.
- Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway.

Procedure

1 On the **SSL VPN-Plus** tab, click **Private Networks**.

2 Click the **Add** () button.

3 Configure the private network settings.

Option	Action
Network	Type the private network IP address in a CIDR format, such as **192169.1.0/24**.
Description	(Optional) Type a description for the network.
Send Traffic	Specify how you want the VPN client to send the private network and Internet traffic. ■ **Over Tunnel** The VPN client sends the private network and Internet traffic over the SSL VPN-Plus enabled edge gateway. ■ **Bypass Tunnel** The VPN client bypasses the edge gateway and sends the traffic directly to the private server.

Option	Action
Enable TCP Optimization	(Optional) To best optimize the Internet speed, when you select **Over Tunnel** for sending the traffic, you must also select **Enable TCP Optimization** Selecting this option enhances the performance of TCP packets within the VPN tunnel but does not improve performance of UDP traffic. Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the Internet. This conventional method encapsulates application layer data in two separate TCP streams. When packet loss occurs, which can happen even under optimal Internet conditions, a performance degradation effect called TCP-over-TCP meltdown occurs. In TCP-over-TCP meltdown, two TCP instruments correct the same single packet of IP data, undermining network throughput and causing connection timeouts. Selecting **Enable TCP Optimization** eliminates the risk of this TCP-over-TCP problem occurring. **Note** When you enable TCP optimization: ■ You must enter the port numbers for which to optimize the Internet traffic. ■ The SSL VPN server opens the TCP connection on behalf of the VPN client. When the SSL VPN server opens the TCP connection, the first automatically generated edge firewall rule is applied, which allows all connections opened from the edge gateway to get passed. Traffic that is not optimized is evaluated by the regular edge firewall rules. The default generated TCP rule is to allow any connections.
Ports	When you select **Over Tunnel**, type a range of port numbers that you want opened for the remote user to access the internal servers, such as **`20–21`** for FTP traffic and **`80–81`** for HTTP traffic. To give unrestricted access to users, leave the field blank.
Status	Enable or disable the private network.

4 Click **Keep**.

5 Click **Save changes** to save the configuration to the system.

What to do next

Add an authentication server. See Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway.

Important Add the corresponding firewall rules to allow network traffic to the private networks you have added in this screen. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule.

Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway

Use the **Authentication** screen on the **SSL VPN-Plus** tab to set up a local authentication server for the edge gateway SSL VPN service and optionally enable client certificate authentication. This authentication server is used to authenticate the connecting users. All users configured in the local authentication server will be authenticated.

You can have only one local SSL VPN-Plus authentication server configured on the edge gateway. If you click **+ LOCAL** and specify additional authentication servers, an error message is displayed when you try to save the configuration.

The maximum time to authenticate over SSL VPN is three (3) minutes. This maximum is determined by the non-authentication timeout, which is 3 minutes by default and is not configurable. As a result, if you have multiple authentication servers in chain authorization and user authentication takes more than 3 minutes, the user will not be authenticated.

Prerequisites

- Navigate to the SSL-VPN Plus Screen.
- Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway.
- If you intend to enable client certificate authentication, verify that a CA certificate has been added to the edge gateway. See Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification.

Procedure

1. Click the **SSL VPN-Plus** tab and **Authentication**.
2. Click **Local**.

3 Configure the authentication server settings.

a (Optional) Enable and configure the password policy.

Option	Description
Enable password policy	Turn on enforcement of the password policy settings you configure here.
Password Length	Enter the minimum and maximum allowed number of characters for password length.
Minimum no. of alphabets	(Optional) Type the minimum number of alphabetic characters, that are required in the password.
Minimum no. of digits	(Optional) Type the minimum number of numeric characters, that are required in the password.
Minimum no. of special characters	(Optional) Type the minimum number of special characters, such as ampersand (&), hash tag (#), percent sign (%) and so on, that are required in the password.
Password should not contain user ID	(Optional) Enable to enforce that the password must not contain the user ID.
Password expires in	(Optional) Type the maximum number of days that a password can exist before the user must change it.
Expiry notification in	(Optional) Type the number of days prior to the **Password expires in** value at which the user is notified the password is about to expire.

b (Optional) Enable and configure the account lockout policy.

Option	Description
Enable account lockout policy	Turn on enforcement of the account lockout policy settings you configure here.
Retry Count	Enter the number of times a user can try to access their account.
Retry Duration	Enter the time period in minutes in which the user account gets locked on unsuccessful login attempts. For example, if you specify the **Retry Count** as 5 and **Retry Duration** as 1 minute, the account of the user is locked after 5 unsuccessful login attempts within 1 minute.
Lockout Duration	Enter the time period for which the user account remains locked. After this time has elapsed, the account is automatically unlocked.

c In the Status section, enable this authentication server.

d (Optional) Configure secondary authentication.

Options	Description
Use this server for secondary authentication	(Optional) Specify whether to use the server as the second level of authentication.
Terminate session if authentication fails	(Optional) Specify whether to end the VPN session when authentication fails.

e Click **Keep**.

4 (Optional) To enable client certification authentication, click **Change certificate**, then turn on the enablement toggle, select the CA certificate to use, and click **OK**.

What to do next

Add local users to the local authentication server so that they can connect with SSL VPN-Plus. See Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server.

Create an installation package containing the SSL Client so remote users can install it on their local systems. See Add an SSL VPN-Plus Client Installation Package.

Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server

Use the **Users** screen on the **SSL VPN-Plus** tab to add accounts for your remote users to the local authentication server for the edge gateway SSL VPN service.

Note If a local authentication server is not already configured, adding a user on the **Users** screen automatically adds a local authentication server with default values. You can then use the edit button on the **Authentication** screen to view and edit the default values. For information about using the **Authentication** screen, see Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway.

Prerequisites

Navigate to the SSL-VPN Plus Screen.

Procedure

1 On the **SSL VPN-Plus** tab, click **Users**.

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

3 Configure the following options for the user.

Option	Description
User ID	Enter the user ID.
Password	Enter a password for the user.
Retype Password	Reenter the password.
First name	(Optional) Enter the first name of the user.
Last name	(Optional) Enter the last name of the user.
Description	(Optional) Enter a description for the user.
Enabled	Specify whether the user is enabled or disabled.
Password never expires	(Optional) Specify whether to keep the same password for this user forever.
Allow change password	(Optional) Specify whether to let the user change the password.
Change password on next login	(Optional) Specify whether you want this user to change the password the next time the user logs in.

4 Click **Keep**.

5 Repeat the steps to add additional users.

What to do next

Add local users to the local authentication server so that they can connect with SSL VPN-Plus. See Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server.

Create an installation package containing the SSL Client so the remote users can install it on their local systems. See Add an SSL VPN-Plus Client Installation Package.

Add an SSL VPN-Plus Client Installation Package

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

You can add an SSL VPN-Plus client installation package to the edge gateway. New users are prompted to download and install this package when they log in to use the VPN connection for the first time. When added, these client installation packages are then downloadable from the FQDN of the edge gateway's public interface.

You can create installation packages that run on Windows, Linux, and Mac operating systems. If you require different installation parameters per SSL VPN client, create an installation package for each configuration.

Prerequisites

Navigate to the SSL-VPN Plus Screen

Procedure

1 On the **SSL VPN-Plus** tab in the tenant portal, click **Installation Packages**.

2 Click the **Add** () button.

3 Configure the installation package settings.

Option	Description
Profile Name	Enter a profile name for this installation package. This name is displayed to the remote user to identify this SSL VPN connection to the edge gateway.
Gateway	Enter the IP address or FQDN of the edge gateway public interface. The IP address or FQDN that you enter is bound to the SSL VPN client. When the client is installed on the local system of the remote user, this IP address or FQDN is displayed on that SSL VPN client. To bind additional edge gateway uplink interfaces to this SSL VPN client, click the **Add** () button to add rows and type in their interface IP addresses or FQDNs, and ports.
Port	(Optional) To modify the port value from the displayed default, double-click the value and enter a new value.

Option	Description
Windows **Linux** **Mac**	Select the operating systems for which you want to create the installation packages.
Description	(Optional) Type a description for the user.
Enabled	Specify whether this package is enabled or disabled.

4 Select the installation parameters for Windows.

Option	Description
Start client on logon	Starts the SSL VPN client when the remote user logs in to their local system.
Allow remember password	Enables the client to remember the user password.
Enable silent mode installation	Hides installation commands from remote users.
Hide SSL client network adapter	Hides the VMware SSL VPN-Plus Adapter which is installed on the computer of the remote user, together with the SSL VPN client installation package.
Hide client system tray icon	Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
Create desktop icon	Creates an icon on the user desktop to invoke the SSL client.
Enable silent mode operation	Hides the window that indicates that installation is complete.
Server security certificate validation	The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.

5 Click **Keep**.

What to do next

Edit the client configuration. See Edit SSL VPN-Plus Client Configuration.

Edit SSL VPN-Plus Client Configuration

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

Prerequisites

Navigate to the SSL-VPN Plus Screen

Procedure

1 On the **SSL VPN-Plus** tab, click **Client Configuration**.

2 Select the **Tunneling mode**.

- In split tunnel mode, only the VPN traffic flows through the edge gateway.
- In full tunnel mode, the edge gateway becomes the default gateway for the remote user and all traffic, such as VPN, local, and Internet, flows through the edge gateway.

3 If you select full tunnel mode, enter the IP address for the default gateway used by the clients of the remote users and, optionally, select whether to exclude local subnet traffic from flowing through the VPN tunnel.

4 (Optional) Disable auto reconnect.

Enable auto reconnect is enabled by default. If auto reconnect is enabled, the SSL VPN client automatically reconnects users when they get disconnected.

5 (Optional) Optionally enable the ability for the client to notify remote users when a client upgrade is available.

This option is disabled by default. If you enable this option, remote users can choose to install the upgrade.

6 Click **Save changes**.

Customize the General SSL VPN-Plus Settings for an Edge Gateway

By default, the system sets some SSL VPN-Plus settings on an edge gateway in your vCloud Director environment. You can use the **General Settings** screen on the **SSL VPN-Plus** tab in the vCloud Director tenant portal to customize these settings.

Prerequisites

Navigate to the SSL-VPN Plus Screen.

Procedure

1 On the **SSL VPN-Plus** tab, click **General Settings**.

2 Edit the general settings as required for the needs of your organization.

Option	Description
Prevent multiple logon using same username	Turn on to restrict a remote user to having only one active login session under the same user name.
Compression	Turn on to enable TCP-based intelligent data compression and improve data transfer speed.
Enable Logging	Turn on to maintain a log of the traffic that passes through the SSL VPN gateway. Logging is enabled by default.
Force virtual keyboard	Turn on to require remote users to use a virtual (on-screen) keyboard only to enter login information.
Randomize keys of virtual keyboard	Turn on to have the virtual keyboard use a randomized key layout.
Session idle timeout	Enter the session idle timeout in minutes. If there is no activity in a user session for the specified time period, the system disconnects the user session. The system default is 10 minutes.
User notification	Type the message to be displayed to remote users after they log in.
Enable public URL access	Turn on to allow remote users to access sites that are not explicitly configured by you for remote user access.

Option	Description
Enable forced timeout	Turn on to have the system disconnect remote users after the time period that you specify in the **Forced timeout** field is over.
Forced timeout	Type the timeout period in minutes. This field is displayed when **Enable forced timeout** toggle is turned on.

3 Click **Save changes**.

Configure IPsec VPN

The edge gateways in a vCloud Director environment support site-to-site Internet Protocol Security (IPsec) to secure VPN tunnels between organization virtual data center networks or between an organization virtual data center network and an external IP address. You can configure the IPsec VPN service on an edge gateway.

Setting up an IPsec VPN connection from a remote network to your organization virtual data center is the most common scenario. The NSX software provides an edge gateway IPsec VPN capabilities, including support for certificate authentication, preshared key mode, and IP unicast traffic between itself and remote VPN routers. You can also configure multiple subnets to connect through IPsec tunnels to the internal network behind an edge gateway. When you configure multiple subnets to connect through IPsec tunnels to the internal network, those subnets and the internal network behind the edge gateway must not have address ranges that overlap.

Note If the local and remote peer across an IPsec tunnel have overlapping IP addresses, traffic forwarding across the tunnel might not be consistent depending on whether local connected routes and auto-plumbed routes exist.

The following IPsec VPN algorithms are supported:

- AES (AES128-CBC)
- AES256 (AES265-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman group 2)
- DH-5 (Diffie-Hellman group 5)
- DH-14 (Diffie-Hellman group 14)

Note Dynamic routing protocols are not supported with IPsec VPN. When you configure an IPsec VPN tunnel between an edge gateway of the organization virtual data center and a physical gateway VPN at a remote site, you cannot configure dynamic routing for that connection. The IP address of that remote site cannot be learned by dynamic routing on the edge gateway uplink.

As described in the *IPSec VPN Overview* topic in the *NSX Administration Guide*, the maximum number of tunnels supported on an edge gateway is determined by its configured size: compact, large, x-large, quad large.

To view the size of your edge gateway configuration, navigate to the edge gateway and click the edge gateway name.

Configuring IPsec VPN on an edge gateway is a multi-step process.

Note If a firewall is between the tunnel endpoints, after you configure the IPsec VPN service, update the firewall rules to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Procedure

1 Navigate to the IPsec VPN Screen

In the **IPsec VPN** screen, you can begin configuring the IPsec VPN service for an NSX Data Center for vSphere edge gateway.

2 Configure the IPsec VPN Site Connections for the Edge Gateway

Use the **IPsec VPN Sites** screen in the vCloud Director tenant portal to configure settings needed to create an IPsec VPN connection between your organization virtual data center and another site using the edge gateway IPsec VPN capabilities.

3 Enable the IPsec VPN Service on an Edge Gateway

When at least one IPsec VPN connection is configured, you can enable the IPsec VPN service on the edge gateway.

4 Specify Global IPsec VPN Settings

Use the **Global Configuration** screen to configure IPsec VPN authentication settings at an edge gateway level. On this screen, you can set a global pre-shared key and enable certification authentication.

Navigate to the IPsec VPN Screen

In the **IPsec VPN** screen, you can begin configuring the IPsec VPN service for an NSX Data Center for vSphere edge gateway.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Navigate to **VPN > IPsec VPN**.

What to do next

Use the **IPsec VPN Sites** screen to configure an IPsec VPN connection. At least one connection must be configured before you can enable the IPsec VPN service on the edge gateway. See Configure the IPsec VPN Site Connections for the Edge Gateway.

Configure the IPsec VPN Site Connections for the Edge Gateway

Use the **IPsec VPN Sites** screen in the vCloud Director tenant portal to configure settings needed to create an IPsec VPN connection between your organization virtual data center and another site using the edge gateway IPsec VPN capabilities.

When you configure an IPsec VPN connection between sites, you configure the connection from the point of view of your current location. Setting up the connection requires that you understand the concepts in the context of the vCloud Director environment so that you configure the VPN connection correctly.

- The local and peer subnets specify the networks to which the VPN connects. When you specify these subnets in the configurations for IPsec VPN sites, enter a network range and not a specific IP address. Use CIDR format, such as `192.168.99.0/24`.
- The peer ID is an identifier that uniquely identifies the remote device that terminates the VPN connection, typically its public IP address. For peers using certificate authentication, this ID must be the distinguished name set in the peer certificate. For PSK peers, this ID can be any string. An NSX best practice is to use the public IP address of the remote device or FQDN as the peer ID. If the peer IP address is from another organization virtual data center network, you enter the native IP address of the peer. If NAT is configured for the peer, you enter the peer's private IP address.
- The peer endpoint specifies the public IP address of the remote device to which you are connecting. The peer endpoint might be a different address from the peer ID if the peer's gateway is not directly accessible from the Internet, but connects through another device. If NAT is configured for the peer, you enter the public IP address that the devices uses for NAT.
- The local ID specifies the public IP address of the edge gateway of the organization virtual data center. You can enter an IP address or hostname along with the edge gateway firewall.
- The local endpoint specifies the network in your organization virtual data center on which the edge gateway transmits. Typically the external network of the edge gateway is the local endpoint.

Prerequisites

- Navigate to the IPsec VPN Screen.
- Configure IPsec VPN.
- If you intend to use a global certificate as the authentication method, verify that certificate authentication is enabled on the **Global Configuration** screen. See Specify Global IPsec VPN Settings.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 On the **IPsec VPN** tab, click **IPsec VPN Sites**.

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

4 Configure the IPsec VPN connection settings.

Option	Action
Enabled	Enable this connection between the two VPN endpoints.
Enable perfect forward secrecy (PFS)	Enable this option to have the system generate unique public keys for all IPsec VPN sessions your users initiate. Enabling PFS ensures that the system does not create a link between the edge gateway private key and each session key. The compromise of a session key will not affect data other than the data exchanged in the specific session protected by that particular key. Compromise of the server's private key cannot be used to decrypt archived sessions or future sessions. When PFS is enabled, IPsec VPN connections to this edge gateway experience a slight processing overhead. **Important** The unique session keys must not be used to derive any additional keys. Also, both sides of the IPsec VPN tunnel must support PFS for it to work.
Name	(Optional) Enter a name for the connection.
Local ID	Enter the external IP address of the edge gateway instance, which is the public IP address of the edge gateway. The IP address is the one used for the peer ID in the IPsec VPN configuration on the remote site.
Local Endpoint	Enter the network that is the local endpoint for this connection. The local endpoint specifies the network in your organization virtual data center on which the edge gateway transmits. Typically, the external network is the local endpoint. If you add an IP-to-IP tunnel using a pre-shared key, the local ID and local endpoint IP can be the same.
Local Subnets	Enter the networks to share between the sites and use a comma as a separator to enter multiple subnets. Enter a network range (not a specific IP address) by entering the IP address using CIDR format. For example, **`192.168.99.0/24`**.

Option	Action
Peer ID	Enter a peer ID to uniquely identify the peer site. The peer ID is an identifier that uniquely identifies the remote device that terminates the VPN connection, typically its public IP address. For peers using certificate authentication, the ID must be the distinguished name in the peer's certificate. For PSK peers, this ID can be any string. An NSX best practice is to use the remote device's public IP address or FQDN as the peer ID. If the peer IP address is from another organization virtual data center network, you enter the native IP address of the peer. If NAT is configured for the peer, you enter the peer's private IP address.
Peer Endpoint	Enter the IP address or FQDN of the peer site, which is the public-facing address of the remote device to which you are connecting. **Note** When NAT is configured for the peer, enter the public IP address that the device uses for NAT.
Peer Subnets	Enter the remote network to which the VPN connects and use a comma as a separator to enter multiple subnets. Enter a network range (not a specific IP address) by entering the IP address using CIDR format. For example, **`192.168.99.0/24`**.
Encryption Algorithm	Select the encryption algorithm type from the drop-down menu. **Note** The encryption type you select must match the encryption type configured on the remote site VPN device.
Authentication	Select an authentication. The options are: ■ **PSK** Pre Shared Key (PSK) specifies that the secret key shared between the edge gateway and the peer site is to be used for authentication. ■ **Certificate** Certificate authentication specifies that the certificate defined at the global level is to be used for authentication. This option is not available unless you have configured the global certificate on the **IPsec VPN** tab's **Global Configuration** screen.
Change Shared Key	(Optional) When you are updating the settings of an existing connection, you can turn on this option on to make the **Pre-Shared Key** field available so that you can update the shared key.
Pre-Shared Key	If you selected **PSK** as the authentication type, type an alphanumeric secret string which can be a string with a maximum length of 128 bytes. **Note** The shared key must match the key that is configured on the remote site VPN device. A best practice is to configure a shared key when anonymous sites will connect to the VPN service.
Display Shared Key	(Optional) Enable this option to make the shared key visible in the screen.

Option	Action
Diffie-Hellman Group	Select the cryptography scheme that allows the peer site and this edge gateway to establish a shared secret over an insecure communications channel. **Note** The Diffie-Hellman Group must match what is configured on the remote site VPN device.
Extension	(Optional) Type one of the following options: ■ `securelocaltrafficbyip=`*IPAddress* to redirect the edge gateway local traffic over the IPsec VPN tunnel. This is the default value. ■ `passthroughSubnets=`*PeerSubnetIPAddress* to support overlapping subnets.

5 Click **Keep**.

6 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

Configure the connection for the remote site. You must configure the IPsec VPN connection on both sides of the connection: your organization virtual data center and the peer site.

Enable the IPsec VPN service on this edge gateway. When at least one IPsec VPN connection is configured, you can enable the service. See Enable the IPsec VPN Service on an Edge Gateway.

Enable the IPsec VPN Service on an Edge Gateway

When at least one IPsec VPN connection is configured, you can enable the IPsec VPN service on the edge gateway.

Prerequisites

- Navigate to the IPsec VPN Screen.
- Verify that at least one IPsec VPN connection is configured for this edge gateway. See the steps described in Configure the IPsec VPN Site Connections for the Edge Gateway.

Procedure

1 On the **IPsec VPN** tab, click **Activation Status**.

2 Click **IPsec VPN Service Status** to enable the IPsec VPN service.

3 Click **Save changes**.

The edge gateway IPsec VPN service is active.

Specify Global IPsec VPN Settings

Use the **Global Configuration** screen to configure IPsec VPN authentication settings at an edge gateway level. On this screen, you can set a global pre-shared key and enable certification authentication.

A global pre-shared key is used for those sites whose peer endpoint is set to **any**.

Prerequisites

- If you intend to enable certificate authentication, verify that you have at least one service certificate and corresponding CA-signed certificates in the **Certificates** screen. Self-signed certificates cannot be used for IPsec VPNs. See Add a Service Certificate to the Edge Gateway.
- Navigate to the IPsec VPN Screen.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. On the **IPsec VPN** tab, click **Global Configuration**.
3. (Optional) Set a global pre-shared key:
   a. Enable the **Change Shared Key** option.
   b. Enter a pre-shared key.

      The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to *any*. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.
   c. (Optional) Optionally enable **Display Shared Key** to make the pre-shared key visible.
   d. Click **Save changes**.
4. Configure certification authentication:
   a. Turn on **Enable Certificate Authentication**.
   b. Select the appropriate service certificates, CA certificates, and CRLs.
   c. Click **Save changes**.

What to do next

You can optionally enable logging for the IPsec VPN service of the edge gateway. See Statistics and Logs for an Edge Gateway.

Configure L2 VPN

The edge gateways in a vCloud Director environment support L2 VPN. With L2 VPN, you can extend your organization virtual data center by enabling virtual machines to maintain network connectivity while retaining the same IP address across geographical boundaries. You can configure the L2 VPN service on an edge gateway.

NSX Data Center for vSphere provides the L2 VPN capabilities of an edge gateway. With L2 VPN, you can configure a tunnel between two sites. Virtual machines remain on the same subnet despite being moved between these sites, which enables you to extend your organization virtual data center by stretching its network using L2 VPN. An edge gateway at one site can provide all services to virtual machines on the other site.

To create the L2 VPN tunnel, you configure an L2 VPN server and L2 VPN client. As described in the *NSX Administration Guide*, the L2 VPN server is the destination edge gateway and the L2 VPN client is the source edge gateway. After configuring the L2 VPN settings on each edge gateway, you must then enable the L2 VPN service on both the server and the client.

Note A routed organization virtual data center network created as a subinterface must exist on the edge gateways.

Navigate to the L2 VPN Screen

To begin configuring the L2 VPN service for an NSX Data Center for vSphere edge gateway, you must navigate to the **L2 VPN** screen.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Navigate to **VPN > L2 VPN**.

What to do next

Configure the L2 VPN server. See Configure the Edge Gateway as an L2 VPN Server.

Configure the Edge Gateway as an L2 VPN Server

The L2 VPN server is the destination NSX edge to which the L2 VPN client is going to connect.

As described in the *NSX Administration Guide*, you can connect multiple peer sites to this L2 VPN server.

Note Changing site configuration settings causes the edge gateway to disconnect and reconnect all existing connections.

Prerequisites

- Verify that the edge gateway has a routed organization virtual data center network that is configured as a subinterface on the edge gateway.
- Navigate to the L2 VPN Screen.
- If you want to bind a service certificate to the L2 VPN connection, verify that the server certificate has already been uploaded to the edge gateway. See Add a Service Certificate to the Edge Gateway.

- You must have the listener IP of the server, listener port, encryption algorithm, and at least one peer site configured before you can enable the L2 VPN service.

Procedure

1. On the **L2 VPN** tab, select **Server** for the L2 VPN mode.
2. On the **Server Global** tab, configure the L2 VPN server's global configuration details.

Option	Action
Listener IP	Select the primary or secondary IP address of an external interface of the edge gateway.
Listener Port	Edit the displayed value as appropriate for the needs of your organization. The default port for the L2 VPN service is 443.
Encryption Algorithm	Select the encryption algorithm for the communication between the server and the client.
Service Certificate Details	Click **Change server certificate** to select the certificate to be bound to the L2 VPN server. In the **Change Server Certificate** window, turn on **Validate Server Certificate**, select a server certificate from the list, and click **OK**.

3. To configure the peer sites, click the **Server Sites** tab.
4. Click the **Add** () button.
5. Configure the settings for an L2 VPN peer site.

Option	Action
Enabled	Enable this peer site.
Name	Enter a unique name for the peer site.
Description	(Optional) Type a description.
User ID **Password** **Confirm Password**	Enter the user name and password with which the peer site is to be authenticated. User credentials on the peer site must be the same as the credentials on the client side.
Stretched Interfaces	Select at least one subinterface to be stretched with the client. The subinterfaces available for selection are those organization virtual data center networks configured as subinterfaces on the edge gateway.
Egress Optimization Gateway Address	(Optional) If the default gateway for virtual machines is the same across the two sites, enter the gateway IP addresses of the subinterfaces for which you want the traffic locally routed or blocked over the L2 VPN tunnel.

6. Click **Keep**.
7. Click **Save changes**.

   The save operation can take a minute to complete.

What to do next

Enable the L2 VPN service on this edge gateway. See Enable the L2 VPN Service on an Edge Gateway.

Configure the Edge Gateway as an L2 VPN Client

The L2 VPN client is the source NSX edge that initiates communication with the destination NSX edge, the L2 VPN server.

Prerequisites

- Navigate to the L2 VPN Screen.
- If this L2 VPN client is connecting to an L2 VPN server that uses a server certificate, verify that the corresponding CA certificate is uploaded to the edge gateway to enable server certificate validation for this L2 VPN client. See Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification.

Procedure

1. On the **L2 VPN** tab, select **Client** for the L2 VPN mode.
2. On the **Client Global** tab, configure the global configuration details of the L2 VPN client.

Option	Description
Server Address	Enter the IP address of the L2 VPN server to which this client is to be connected.
Server Port	Enter the L2 VPN server port to which the client should connect. The default port is 443.
Encryption Algorithm	Select the encryption algorithm for communicating with the server.
Stretched Interfaces	Select the subinterfaces to be stretched to the server. The subinterfaces available to select are the organization virtual data center networks configured as subinterfaces on the edge gateway.
Egress Optimization Gateway Address	(Optional) If the default gateway for virtual machines is the same across the two sites, type the gateway IP addresses of the subinterfaces or the IP addresses to which traffic should not flow over the tunnel.
User Details	Enter the user ID and password for authentication with the server.

3. Click **Save changes**.

   The save operation can take a minute to complete.
4. (Optional) To configure advanced options, click the **Client Advanced** tab.
5. If this L2 VPN client edge does not have direct access to the Internet, and must reach the L2 VPN server edge by using a proxy server, specify the proxy settings.

Option	Description
Enable Secure Proxy	Select to enable the secure proxy.
Address	Enter the proxy server IP address.

Option	Description
Port	Enter the proxy server port.
User Name **Password**	Enter the proxy server authentication credentials.

6 To enable server certification validation, click **Change CA certificate** and select the appropriate CA certificate.

7 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

Enable the L2 VPN service on this edge gateway. See Enable the L2 VPN Service on an Edge Gateway.

Enable the L2 VPN Service on an Edge Gateway

When the required L2 VPN settings are configured, you can enable the L2 VPN service on the edge gateway.

Note If HA is already configured on this edge gateway, ensure that the edge gateway has more than one internal interface configured on it. If only a single interface exists and that has already been used by the HA capability, the L2 VPN configuration on the same internal interface fails.

Prerequisites

- If this edge gateway is an L2 VPN server, the destination NSX edge, verify that the required L2 VPN server settings and at least one L2 VPN peer site are configured. See the steps described in Configure the Edge Gateway as an L2 VPN Server.
- If this edge gateway is an L2 VPN client, the source NSX edge, verify that the L2 VPN client settings are configured. See the steps described in Configure the Edge Gateway as an L2 VPN Client.
- Navigate to the L2 VPN Screen.

Procedure

1 On the **L2 VPN** tab, click the **Enable** toggle.

2 Click **Save changes**.

The L2 VPN service of the edge gateway becomes active.

What to do next

Create NAT or firewall rules on the Internet-facing firewall side to enable the L2 VPN server to connect to the L2 VPN client.

Remove the L2 VPN Service Configuration from an Edge Gateway

You can remove the existing L2 VPN service configuration of the edge gateway. This action also disables the L2 VPN service on the edge gateway.

Prerequisites

Navigate to the L2 VPN Screen

Procedure

1. Scroll down to the bottom of the L2 VPN screen, and click **Delete configuration**.
2. To confirm the deletion, click **OK**.

The L2 VPN service is disabled and the configuration details are removed from the edge gateway.

SSL Certificate Management

The NSX software in the vCloud Director environment provides the ability to use Secure Sockets Layer (SSL) certificates with the SSL VPN-Plus and IPsec VPN tunnels you configure for your edge gateways.

The edge gateways in your vCloud Director environment support self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA. Yyou can generate certificate signing requests (CSRs), import the certificates, manage the imported certificates, and create certificate revocation lists (CRLs).

About Using Certificates with Your Organization Virtual Data Center

You can manage certificates for the following networking areas in your vCloud Director organization virtual data center.

- IPsec VPN tunnels between an organization virtual data center network and a remote network.
- SSL VPN-Plus connections between remote users to private networks and web resources in your organization virtual data center.
- An L2 VPN tunnel between two NSX edge gateways.
- The virtual servers and pools servers configured for load balancing in your organization virtual data center

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.

Generate a Certificate Signing Request for an Edge Gateway

Before you can order a signed certificate from a CA or create a self-signed certificate, you must generate a Certificate Signing Request (CSR) for your edge gateway.

A CSR is an encoded file that you need to generate on an NSX edge gateway which requires an SSL certificate. Using a CSR standardizes the way that companies send their public keys together with information that identifies their company names and domain names.

You generate a CSR with a matching private-key file that must remain on the edge gateway. The CSR contains the matching public key and other information such as the name, location, and domain name of your organization.

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 Click the **Certificates** tab.

3 On the **Certificates** tab, click **CSR**.

4 Configure the following options for the CSR:

Option	Description
Common Name	Enter the fully qualified domain name (FQDN) for the organization that you will be using the certificate for (for example, `www.example.com`). Do not include the `http://` or `https://` prefixes in your common name.
Organization Unit	Use this field to differentiate between divisions within your vCloud Director organization with which this certificate is associated. For example, Engineering or Sales.
Organization Name	Enter the name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
Locality	Enter the city or locality where your company is legally registered.
State or Province Name	Enter the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country Code	Enter the country name where your company is legally registered.
Private Key Algorithm	Type the key type, either RSA or DSA, for the certificate. RSA is typically used. The key type defines the encryption algorithm for communication between the hosts. **Note** SSL VPN-Plus supports RSA certificates only.
Key Size	Enter the key size in bits. The minimum is 2048 bits.
Description	(Optional) Enter a description for the certificate.

5 Click **Keep**.

The system generates the CSR and adds a new entry with type CSR to the on-screen list.

In the on-screen list, when you select an entry with type CSR, the CSR details are displayed in the screen. You can copy the displayed PEM formatted data of the CSR and submit it to a certificate authority (CA) to obtain a CA-signed certificate.

What to do next

Use the CSR to create a service certificate using one of these two options:

- Transmit the CSR to a CA to obtain a CA-signed certificate. When the CA sends you the signed certificate, import the signed certificate into the system. See Import the CA-Signed Certificate Corresponding to the CSR Generated for an Edge Gateway.
- Use the CSR to create a self-signed certificate. See Configure a Self-Signed Service Certificate.

Import the CA-Signed Certificate Corresponding to the CSR Generated for an Edge Gateway

After you generate a Certificate Signing Request (CSR) and obtain the CA-signed certificate based on that CSR, you can import the CA-signed certificate to use it by your edge gateway.

Prerequisites

Verify that you obtained the CA-signed certificate that corresponds to the CSR. If the private key in the CA-signed certificate does not match the one for the selected CSR, the import process fails.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Click the **Certificates** tab.

3 Select the CSR in the on-screen table for which you are importing the CA-signed certificate.

4 Import the signed certificate.

a Click **Signed certificate generated for CSR**.

b Provide the PEM data of the CA-signed certificate.

- If the data is in a PEM file on a system you can navigate to, click the **Upload** button to browse to the file and select it.
- If you can copy and paste the PEM data, paste it into the **Signed Certificate (PEM format)** field.

  Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

c (Optional) Type a description.

d Click **Keep**.

Note If the private key in the CA-signed certificate does not match the one for the CSR you selected on the Certificates screen, the import process fails.

The CA-signed certificate with type Service Certificate appears in the on-screen list.

What to do next

Attach the CA-signed certificate to your SSL VPN-Plus or IPsec VPN tunnels as required. See Configure SSL VPN Server Settings and Specify Global IPsec VPN Settings.

Configure a Self-Signed Service Certificate

You can configure self-signed service certificates with your edge gateways, to use in their VPN-related capabilities. You can create, install, and manage self-signed certificates.

If the service certificate is available on the Certificates screen, you can specify that service certificate when you configure the VPN-related settings of the edge gateway. The VPN presents the specified service certificate to the clients accessing the VPN.

Prerequisites

Verify that at least one CSR is available on the **Certificates** screen for the edge gateway. See Generate a Certificate Signing Request for an Edge Gateway.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Click the **Certificates** tab.

3 Select the CSR in the list that you want to use for this self-signed certificate and click **Self-sign CSR**.

4 Type the number of days that the self-signed certificate is valid for.

5 Click **Keep**.

The system generates the self-signed certificate and adds a new entry with type Service Certificate to the on-screen list.

The self-signed certificate is available on the edge gateway. In the on-screen list, when you select an entry with type Service Certificate, its details are displayed in the screen.

Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification

Adding a CA certificate to an edge gateway enables trust verification of SSL certificates that are presented to the edge gateway for authentication, typically the client certificates used in VPN connections to the edge gateway.

You usually add the root certificate of your company or organization as a CA certificate. A typical use is for SSL VPN, where you want to authenticate VPN clients using certificates. Client certificates can be distributed to the VPN clients and when the VPN clients connect, their client certificates are validated against the CA certificate.

Note When adding a CA certificate, you typically configure a relevant Certificate Revocation List (CRL). The CRL protects against clients that present revoked certificates. See Add a Certificate Revocation List to an Edge Gateway.

Prerequisites

Verify that you have the CA certificate data in PEM format. In the user interface, you can either paste in the PEM data of the CA certificate or browse to a file that contains the data and is available in your network from your local system.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. Click the **Certificates** tab.
3. Click **CA certificate**.
4. Provide the CA certificate data.
   - If the data is in a PEM file on a system you can navigate to, click the **Upload** button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **CA Certificate (PEM format)** field.

     Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.
5. (Optional) Type a description.
6. Click **Keep**.

The CA certificate with type CA Certificate appears in the on-screen list. This CA certificate is now available for you to specify when you configure the VPN-related settings of the edge gateway.

Add a Certificate Revocation List to an Edge Gateway

A Certificate Revocation List (CRL) is a list of digital certificates that the issuing Certificate Authority (CA) claims to be revoked, so that systems can be updated not to trust users that present those revoked certificates. You can add CRLs to the edge gateway.

As described in the *NSX Administration Guide*, the CRL contains the following items:

- The revoked certificates and the reasons for revocation
- The dates that the certificates are issued
- The entities that issued the certificates
- A proposed date for the next release

When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

Procedure

1. Open Edge Gateway Services.
   a. Navigate to **Networking** > **Edges**.
   b. Select the edge gateway to edit, and click **Services**.
2. Click the **Certificates** tab.
3. Click **CRL**.
4. Provide the CRL data.
   - If the data is in a PEM file on a system you can navigate to, click the **Upload** button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **CRL (PEM format)** field.

     Include the `-----BEGIN X509 CRL-----` and `-----END X509 CRL-----` lines.
5. (Optional) Type a description.
6. Click **Keep**.

The CRL appears in the on-screen list.

Add a Service Certificate to the Edge Gateway

Adding service certificates to an edge gateway makes those certificates available for use in the VPN-related settings of the edge gateway. You can add a service certificate to the **Certificates** screen.

Prerequisites

Verify that you have the service certificate and its private key in PEM format. In the user interface, you can either paste in the PEM data or browse to a file that contains the data and is available in your network from your local system.

Procedure

1 Open Edge Gateway Services.
   a Navigate to **Networking** > **Edges**.
   b Select the edge gateway to edit, and click **Services**.
2 Click the **Certificates** tab.
3 Click **Service certificate**.
4 Input the PEM-formatted data of the service certificate.
   - If the data is in a PEM file on a system you can navigate to, click the **Upload** button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **Service Certificate (PEM format)** field.

     Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.
5 Input the PEM-formatted data of the certificate private key.
   - If the data is in a PEM file on a system you can navigate to, click the **Upload** button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **Private Key (PEM format)** field.

     Include the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.
6 Enter a private key passphrase and confirm it.
7 (Optional) Type a description.
8 Click **Keep**.

The certificate with type Service Certificate appears in the on-screen list. This service certificate is now available for you to select when you configure the VPN-related settings of the edge gateway.

Custom Grouping Objects

The NSX software in your vCloud Director environment provides the capability for defining sets and groups of certain entities, which you can then use when specifying other network-related configurations, such as in firewall rules.

Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration

An IP set is a group of IP addresses that you can create at an organization virtual data center level. You can use an IP set as the source or destination in a firewall rule or in a DHCP relay configuration.

You create an IP set by using the **Grouping Objects** page of the vCloud Director tenant portal. The **Grouping Object**s page is available on both the Services and Edge Gateway screens.

Procedure

1 Open the Grouping Objects page.

Option	Action
Open through Edge Gateway Services	a Navigate to **Networking > Edges**. b Select the edge gateway to edit, and click **Configure Services**. c Click **Grouping Objects**.
Open through Security Services	a Navigate to **Networking > Security**. b Select the security service to edit, and click **Configure Services**. c Click **Grouping Objects**.

2 Click the **IP Sets** tab.

The IP sets that are already defined are displayed on the screen.

3 To add an IP set, click the **Create** () button.

4 Enter a name, optionally, a description for the IP set, and the IP addresses to be included in the set.

5 (Optional) If you are specifying the IP set using the **Grouping Objects** page on the Services screen, use the **Inheritance** toggle to enable inheritance and allow visibility at the underlying scopes.

Inheritance is enabled by default.

6 To save this IP set, click **Keep**.

The new IP set is available for selection as the source or destination in firewall rules or in DHCP relay configurations.

Create a MAC Set for Use in Firewall Rules

An MAC set is a group of MAC addresses that you can create at an organization virtual data center level. You can use a MAC set as the source or destination in a firewall rule.

You create a MAC set using the **Grouping Objects** page of the vCloud Director tenant portal. The Grouping Objects page is available on both the **Services** and **Edge Gateway** screens.

Procedure

1 Open the Grouping Objects page.

Option	Action
Open through Edge Gateway Services	a Navigate to **Networking > Edges**. b Select the edge gateway to edit, and click **Configure Services**. c Click **Grouping Objects**.
Open through Security Services	a Navigate to **Networking > Security**. b Select the security service to edit, and click **Configure Services**. c Click **Grouping Objects**.

2 Click the **MAC Sets** tab.

The MAC sets that are already defined are displayed on the screen.

3 To add a MAC set, click the **Create** () button.

4 Enter a name for the set, optionally, a description, and the MAC addresses to be included in the set.

5 (Optional) If you are specifying the MAC set using the **Grouping Objects** page on the **Services** screen, use the **Inheritance** toggle to enable inheritance and allow visibility at underlying scopes.

Inheritance is enabled by default.

6 To save the MAC set, click **Keep**.

The new MAC set is available for selection as the source or destination in firewall rules.

View Services Available for Firewall Rules

You can view the list of services that are available for use in firewall rules. In this context, a service is a protocol-port combination.

You can view the available services using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Services and Edge Gateway screens.

You cannot add new services to the list using the tenant portal. The set of services available for your use is managed by your vCloud Director system administrator.

Procedure

1 Open the Grouping Objects page.

Option	Action
Open through Edge Gateway Services	a Navigate to **Networking > Edges**. b Select the edge gateway to edit, and click **Configure Services**. c Click **Grouping Objects**.
Open through Security Services	a Navigate to **Networking > Security**. b Select the security service to edit, and click **Configure Services**. c Click **Grouping Objects**.

2 Click the **Services** tab.

The available services are displayed on the screen.

View Service Groups Available for Firewall Rules

You can view the list of service groups that are available for use in firewall rules. In this context, a service is a protocol-port combination, and a service group is a group of services or other service groups.

You can view the available service groups using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Services and Edge Gateway screens.

You cannot create service groups using the tenant portal. The set of service groups available for your use is managed by your vCloud Director system administrator.

Procedure

1 Open the Grouping Objects page.

Option	Action
Open through Edge Gateway Services	a Navigate to **Networking > Edges**. b Select the edge gateway to edit, and click **Configure Services**. c Click **Grouping Objects**.
Open through Security Services	a Navigate to **Networking > Security**. b Select the security service to edit, and click **Configure Services**. c Click **Grouping Objects**.

2 Click the **Service Groups** tab.

The available service groups are displayed on the screen. The Description column displays the services that are grouped in each service group.

Statistics and Logs for an Edge Gateway

You can view statistics and logs for an edge gateway.

View Statistics

You can view statistics on the **Edge Gateway Services** screen.

Procedure

1 Open Edge Gateway Services.

a Navigate to **Networking** > **Edges**.

b Select the edge gateway to edit, and click **Services**.

2 Click the **Statistics** tab.

3 Navigate through the tabs depending on the type of statistics you want to see.

Option	Description
Connections	The Connections screen provides operational visibility. The screen displays graphs for the traffic flowing through the interfaces of the selected edge gateway and connection statistics for the firewall and load balancer services. Select the period for which you want to view the statistics.
IPsec VPN	The IPsec VPN screen displays the IPsec VPN status and statistics, and status and statistics for each tunnel.
L2 VPN	The L2 VPN screen displays the L2 VPN status and statistics.

Enable Logging

You can enable logging for an edge gateway. In addition to enabling logging for the features for which you want to collect log data, to complete the configuration, you must have a Syslog server to receive the collected log data. When you configure a Syslog server on the Edge Settings screen, you are able to access the logged data from that Syslog server.

Prerequisites

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

Procedure

1 Open Edge Gateway Services.

   a Navigate to **Networking** > **Edges**.

   b Select the edge gateway to edit, and click **Services**.

2 On the **Edge Settings** tab, click the **Edit Syslog server** button.

   You can customize the Syslog server for the networking-related logs of your edge gateway for those services that have logging enabled.

   If the vCloud Director system administrator has already configured a Syslog server for the vCloud Director environment, the system uses that Syslog server by default and its IP address is displayed on the **Edge Settings** screen.

3 Enable logging per feature.

   - On the **NAT** tab, click the **DNAT Rule** button, and turn on the **Enable logging** toggle.

     Logs the address translation.

   - On the **NAT** tab, click the **SNAT Rule** button, and turn on the **Enable logging** toggle.

     Logs the address translation.

   - On the **Routing** tab, click **Routing Configuration**, and under Dynamic Routing Configuration, turn on the **Enable logging** toggle.

     Logs the dynamic routing activities. From the **Log Level** drop-down menu, you can select the lower bound of the message status level to log.

   - On the **Load Balancer** tab, click **Global Configuration**, and turn on the **Enable logging** toggle.

     Logs the traffic flow for the load balancer. From the **Log Level** drop-down menu, you can select the lower bound of the message status level to log.

   - On the **VPN** tab, navigate to **IPSec VPN > Logging Settings**, and turn on the **Enable logging** toggle.

     Logs the traffic flow between the local subnet and peer subnet. From the **Log Level** drop-down menu, you can select the lower bound of the message status level to log.

- On the **SSL VPN-Plus** tab, click **General Settings**, and turn on the **Enable logging** toggle.

  Maintains a log of the traffic passing through the SSL VPN gateway.
- On the **SSL VPN-Plus** tab, click **Server Settings**, and turn on the **Enable logging** toggle.

  Logs the activities that occur on the SSL VPN server, for Syslog. From the **Log Level** drop-down menu, you can select the lower bound of the message status level to log.

Enable SSH Command-Line Access to an Edge Gateway

You can enable SSH command-line access to an edge gateway.

Procedure

1 Open Edge Gateway Services.

  a Navigate to **Networking** > **Edges**.

  b Select the edge gateway to edit, and click **Services**.

2 Click the **Edge Settings** tab.

3 Configure the SSH settings.

Option	Description
Username **Password** **Retype Password**	Enter the credentials for the SSH access to this edge gateway. By default, the SSH user name is **admin**.
Password Expiry	Enter the expiration period for the password, in days.
Login Banner	Enter the text to be displayed to users when they begin an SSH connection to the edge gateway.

4 Turn on the **Enabled** toggle.

What to do next

Configure the appropriate NAT or firewall rules to allow an SSH access to this edge gateway.

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, Create and Assign Security Tags.

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.

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.

Managing NSX-T Data Center Edge Gateways

7

An NSX-T Data Center edge gateway provides a routed organization VDC network with connectivity to external networks and IP management properties. It can also provide services such as firewall, network address translation (NAT), DNS forwarding, and DHCP, which is enabled by default.

This chapter includes the following topics:

Add a Firewall Group to an NSX-T Edge Gateway

To create firewall rules and add them to an NSX-T edge gateway, you must first create the firewall groups. Firewall groups are groups of objects to which the firewall rules apply. Combining multiple objects into firewall groups helps reduce the total number of firewall rules to be created.

Procedure

1. Navigate to **Networking** > **Edges**.
2. Click the NSX-T edge gateway and click **Security**.
3. Click the **Groups** tab and click **New**.
4. Enter a name and, optionally, a description for the firewall group.
5. Enter an IP address or an IP addresses range for the virtual machines that the group includes, and click **Add**.
6. To save the firewall group, click **Save**.

You created a firewall group and added it to the NSX-T edge gateway.

What to do next

Add an NSX-T Edge Gateway Firewall Rule

Add an NSX-T Edge Gateway Firewall Rule

To control the incoming and outgoing network traffic to and from an NSX-T Edge Gateway, you create firewall rules.

Procedure

1 Navigate to **Networking** > **Edges**.

2 Click the edge gateway and click **Services**.

3 If the **Firewall** screen is not already visible, click the **Firewall** tab.

4 Click **Edit Rules**.

5 Select a firewall rule and click the **Add Above** button.

A row for the new rule is added above the selected rule.

6 Configure the firewall rule.

Option	Description
Name	Enter a name for the rule.
State	To enable the rule upon creation, turn on the **State** toggle.
Applications	(Optional) To select a specific port profile to which the rule applies, turn on the **Applications** toggle and click **Save**.
Source	Select an option and click **Keep**. ■ To allow or deny traffic from any source address, turn on the **Any Source** toggle. ■ To allow or deny traffic from specific firewall groups, select the firewall groups from the list.
Destination	Select an option and click **Keep**. ■ To allow or deny traffic to any source address, toggle on **Any Destination** . ■ To allow or deny traffic from specific firewall groups, select the firewall groups from the list.
Action	From the **Action** drop-down menu, select an option. ■ To allow traffic from or to the specified sources, destinations, and services, select **Accept**. ■ To block traffic from or to the specified sources, destinations, and services, select **Deny**.
IP Protocol	Select whether to apply the rule to IPv4 or IPv6 traffic.
Direction	Select the traffic direction to which to apply the rule.
Enable logging.	To have the address translation performed by this rule logged, turn on the **Enable logging** toggle.

7 Click **Save**.

8 To configure additional rules, repeat these steps.

After the firewall rules are created, they appear in the Edge Gateway Firewall Rules list. You can move up, move down, edit, or delete the rules as needed.

Add an SNAT or a DNAT Rule to an NSX-T Edge Gateway

To change the source IP address from a public to a private IP address or the reverse, create a NAT (SNAT) rule. To change the destination IP address from a public to a private IP address or the reverse, create a destination NAT (DNAT) rule.

When you configure a SNAT or a DNAT rule on an edge gateway in the vCloud Director environment, you always configure the rule from the perspective of your organization VDC. A SNAT rule translates the source IP address of packets sent from an organization VDC network out to an external network or to another organization VDC network. A DNAT rule translates the IP address and, optionally, the port of packets received by an organization VDC network that are coming from an external network or from another organization VDC network.

Prerequisites

The public IP addresses must have been added to the edge gateway interface on which you want to add the rule.

Procedure

1 Navigate to **Networking** > **Edges**.

2 Click the edge gateway and click **NAT**.

3 To add a rule, click **Add**.

4 Configure a Source NAT rule (inside going outside).

Option	Description
Name	Enter a name for the rule.
State	To enable the rule upon creation, turn on the **State** toggle.
Interface type	Select the interface on which to apply the rule.
External IP	Enter the IP address or a range of IP addresses of the virtual machines for which you are configuring SNAT, so that they can send traffic to the external network.
Internal IP	Enter the public IP address of the edge gateway for which you are configuring the SNAT rule.
Enable logging.	To have the address translation performed by this rule logged, turn on the **Enable logging** toggle.

5 Configure a Destination NAT rule (outside going inside).

Option	Description
Name	Enter a name for the rule.
State	To enable the rule upon creation, turn on the **State** toggle.

Option	Description
Interface type	Select the interface on which to apply the rule.
External IP	Enter the public IP address of the edge gateway for which you are configuring the DNAT rule. The IP addresses that you enter must belong to the suballocated IP range of the edge gateway.
Application	(Optional) Select a specific application port profile to which to apply the rule. The application port profile includes a port and a protocol that the incoming traffic uses on the edge gateway to connect to the internal network.
Internal IP	Enter the IP address or a range of IP addresses of the virtual machines for which you are configuring DNAT, so that they can receive traffic from the external network.
Internal Port	(Optional) Select the port or port range into which the DNAT rule is translating for the packets inbound to the virtual machines.
Enable logging.	To have the address translation performed by this rule logged, turn on the **Enable logging** toggle.

6 Click **Save**.

7 To configure additional rules, repeat these steps.

Configure a DNS Forwarder Service on an NSX-T Edge Gateway

To forward DNS queries to external DNS servers, configure a DNS forwarder.

As part of your DNS forwarder service configuration, you can also add conditional forwarder zones. A conditional forwarder zone is configured as a list containing up to five FQDN DNS zones. If a DNS query matches a domain name from that list, the query is forwarded to the servers from the corresponding forwarder zone.

Procedure

1 Navigate to **Networking** > **Edges**.

2 Click the edge gateway and click **Services**.

3 Click **DNS**, and in the **DNS Forwarder** section, click **Edit**.

4 To enable the DNS Forwarder service, turn on the **State** toggle.

5 Enter a name and, optionally, a description for the default DNS zone.

6 Enter one or more upstream server IP addresses, separated by a comma.

7 Click **Save**.

8 (Optional) Add a conditional forwarder zone.

   a In the **Conditional Forwarder Zone** section, click **Add**.

   b Enter a name for the forwarder zone.

   c Enter one or more upstream server IP addresses, separated by a comma.

   d Enter one or more domain names, separated by a comma, and click **Save**.

Create Custom Application Port Profiles

To create firewall and NAT rules, you can use preconfigured application port profiles and custom application port profiles.

Application port profiles include a combination of a protocol and a port, or a group of ports, that is used for firewall and NAT services on the edge gateway. In addition to the default port profiles that are preconfigured for NSX-T Data Center, you can create custom application port profiles.

When you create a custom application port profile on an edge gateway, it becomes visible to all the other NSX-T Data Center edge gateways that are in the same organization VDC.

Procedure

1 Navigate to **Networking** > **Edges**.

2 Click the edge gateway and click the **Security** tab.

3 Click **Application Port Profiles**.

4 In the **Custom Applications** section, click **New**.

5 Enter a name and, optionally, a description for the application port profile.

6 Select a protocol from the drop-down menu.

7 Enter a port, or a range of ports, separated by a comma, and click **Save**.

What to do next

Use application port profiles to create firewall and NAT rules. See Add an NSX-T Edge Gateway Firewall Rule and Add an SNAT or a DNAT Rule to an NSX-T Edge Gateway.

Using Named Disks and Reviewing Storage Policies

8

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

This chapter includes the following topics:

Creating and Using Named Disks

Named disks are standalone virtual disks that you create in Organization VDCs. **Organization administrators** and users who have the respective rights can create, remove, and update named disks, and connect them to virtual machines.

When you create a named disk, it is associated with an Organization VDC but not with a virtual machine. After you create the disk in a VDC, the disk owner or an administrator can attach it to any virtual machine deployed in the VDC. The disk owner can also modify the disk properties, detach it from a virtual machine, and remove it from the VDC. **System administrators** and **organization administrators** have the same rights to use and modify the disk as the disk owner.

Create a Named Disk

You can create a named disk and attach it to a virtual machine at a later stage.

To create a named disk, you must specify its name and size. You can optionally include a description and select a storage profile to be used by the disk.

Prerequisites

You must have an **organization administrator** role or disk owner rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and under **Storage**, select **Named Disks** from the left panel.
2. Click **New**.
3. Enter a name and, optionally, a description of the disk.

4 Select the storage policy from the **Storage Policy** drop-down menu.

5 Enter the size of the named disk in bytes.

6 Select the bus type and subtype, from the **Bus Type** and **Bus Sub-Type** drop-down menus, respectively, and click **Save**.

Edit a Named Disk

After you have created the disk, you can modify its name, description, storage policy, and size.

Prerequisites

You must have an **organization administrator** role or disk owner rights.

Procedure

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

2 Select the disk you want to modify, and click **Edit**.

3 Edit the settings such as name, description, storage policy, and size in bytes.

4 Click **Save**.

Attach a Named Disk to a Virtual Machine

After you create a named disk in a VDC, you can attach it to any virtual machine that is deployed in the VDC.

Prerequisites

You must have an **organization administrator** role or disk owner rights.

Procedure

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

2 Click the radio button next to the name of the named disk that you want to attach to a virtual machine, and click **Attach**.

3 From the drop-down menu, select a virtual machine to which to attach the named disk, and click **Apply**.

The named disk is attached to the virtual machine.

What to do next

You can attach more named disks to the VM, or detach them as needed.

Delete a Named Disk

If you don't need a named disk, you can delete it.

Prerequisites

You must have an **organization administrator** role or disk owner rights.

Procedure

1. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore and under **Storage**, select **Named Disks** from the left panel.
2. Select the disk you want to delete, and click **Delete**.
3. Click **OK**.

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

9

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 Dedicated vCenter Server Instances and Proxies 10

Starting with vCloud Director 9.7, you can access a dedicated vCenter Server environment from vCloud Director. vCloud Director can act as an HTTP proxy server and provide access to components from the underlying vSphere environment.

In vCloud Director, a Software-Defined Data Center (SDDC) encapsulates an entire dedicated vCenter Server environment. A dedicated vCenter Server instance can include one or more proxies that provide access to different components from the underlying environment.

The **system administrator** can publish one or more dedicated vCenter Server instances to your organization. You can use the containing proxies to access the UI or API of the proxied components.

This chapter includes the following topics:

Configure Your Browser with Your Proxy Settings

Before you can access the UI of a proxied vSphere component, you must set up the proxies that are published to your organization.

To configure your browser to use your published proxies, you copy the URL of the proxy auto-config (PAC) file into your browser.

Note When the **system administrator** publishes a dedicated vSphere data center to your organization, or adds a proxy to one of your dedicated vSphere data centers, it is possible that it takes a few minutes for the browser to refetch the PAC from the provided URL. To force a refresh of the browser, you can repeat this procedure.

Prerequisites

- The **system administrator** published at least one dedicated and enabled vCenter Server instance to your organization.
- The **system administrator** published the **SDDC_VIEW** right to your organization, and your role includes this right.

- The **system administrator** published and enabled the **CPOM extension** plug-in to your organization. This plug-in provides the function for viewing and using dedicated vSphere data centers in the vCloud Director Tenant Portal.

Procedure

1. From the main menu (☰), select **Datacenters**.
2. On the **Dedicated vSphere Datacenters** pane, click **Click here to view Proxy Configuration Guide**.
3. Copy the PAC URL and click **Next**.
4. Follow the instructions to configure your browser to point to the PAC URL.
5. If a proxied component is using self-signed certificates, import the certificates to your browser.
   a. On the target vSphere data center card, click **Actions**, and click **Import Certificate**.
   b. Download the certificate and the certificate revocation list (CRL).
   c. Import the downloaded certificate to your browser.

      See the user instructions for your browser.

Log In to the UI of a Proxied Component

You can access the UI of a proxied component with your vCloud Director account.

Prerequisites

Before you log in to the UI of a proxied component, you must configure your access to the proxy. See Configure Your Browser with Your Proxy Settings.

Procedure

1. From the main menu (☰), select **Datacenters**.
2. Click the **Dedicated vSphere Datacenters** tab.
3. Open the proxy of the Dedicated vCenter Server instance.
   - To open the default proxy, click **Open vSphere**.
   - To open a non-default proxy, follow these steps:
     - Click **Actions**, and click **View Proxies**.
     - Click the proxy URL.

   A new card with your proxy credentials opens.
4. Copy the user name and the password.
5. To activate the proxy, click **Open**.

   A new card opens and prompts you for authentication against the proxy.

6 In the **User Name** text box, paste the copied user name.

7 In the **Password** text box, paste the copied password and click **OK.**

The UI of the proxied component opens.

Working with vApp Templates

11

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.

Assign a VM Placement Policy and a VM Sizing Policy to a vApp Template

To associate the VMs of a vApp template with specific VM placement and VM sizing policies, you can tag individual VMs of a vApp template with the policies you want to assign.

Starting with vCloud Director 10.0, you can allow the users to change the predefined VM placement or VM sizing policies while editing a VM.

Note After you upgrade to vCloud Director 10.0, all pre-existing template taggings become modifiable. If you want to disallow the changes to the predefined VM placement or VM sizing policies, you must deselect the **Modifiable** check box for the policies that you want to be unchangeable.

Prerequisites

- This operation requires the right to edit a vApp template.
- Verify that you have at least one vApp template in your vCloud Director environment.

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 Select the radio button next to the vApp template you want to tag, and click **Tag with Compute Policies**.

3 If you want to assign a VM placement policy to a VM in the vApp template, select a policy from the **VM Placement Policy** drop-down menu on the row corresponding to the VM.

4 If you want to assign a VM sizing policy to a VM in the vApp template, select a policy from the **VM Sizing Policy** drop-down menu on the row corresponding to the VM.

5 (Optional) To allow the users to change the predefined VM placement or VM sizing policies while editing a VM, select the **Modifiable** check box under the policy drop-down menu.

6 Click **Tag**.

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

12

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

13

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:

- Synchronize a Subscribed Catalog

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

14

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, optionally, an Edge Gateway, 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.

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

15

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 SAML 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 that you Chapter 16 Enable Your Organization to Use a SAML Identity Provider.

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.

   You will only view the source LDAP server or SAML server that you configured as identity provider.

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**.
SAML	Import users from a SAML server. Enter the user names of the users that you want to import. User names must be in the name identifier format supported by the SAML identity provider configured for this organization. **Note** If you are using vCenter Single Sign-On as the SAML identity provider, the user names that you import from a vCenter Single Sign-On domain must be in User Principal Name (UPN) format, for example jdoe@mydomain.com. Use a new line for each user name.

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 enabled your organization to use a SAML identity provider, you can import an LDAP group or a SAML 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 SAML 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 that you Chapter 16 Enable Your Organization to Use a SAML Identity Provider.

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.

You will only view the source LDAP server or SAML server that you configured as identity provider.

Source	Action
LDAP	Import a user group from an LDAP server. a Enter a full or partial name in the text box and click **Search**. b Select the user groups that you want to import and click **Add**.
SAML	Import user groups from a SAML server. Enter the names of the groups that you want to import. Use a new line for each group name.

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 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 15-1. 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 15-1. 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				
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			
Catalog Item: Edit vApp Template / Media	X	X			
Catalog Item: Enable vApp Template / Media Download	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: Enable / Disable Distributed Firewall	X				
Distributed Firewall: View Distributed Firewall Rules	X				
Edge Cluster: View Edge Cluster	X				
Edge Cluster: Manage Edge Cluster	X				
Gateway: Configure Syslog Server	X				
Gateway: Configure System Logging	X				
Gateway: Convert to Advanced Gateway	X				
Gateway: View Gateway	X				
Gateway: Enable Distributed Routing	X				

Table 15-1. 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: Import Edge Gateway	X				
Gateway Services: BGP Routing Configure					
Gateway Services: Configure ECMP Routing	X				
Gateway Services: Configure Edge Gateway DNS	X	X	X	X	X
Gateway Services: DHCP Configure	X				
Gateway Services: Firewall Configure	X				
Gateway Services: IPSEC VPN Configure	X				
Gateway Services: L2 VPN Configure					
Gateway Services: Load Balancer Configure	X				
Gateway Services: NAT Configure	X				
Gateway Services: OSPF Routing Configure	X				
Gateway Services: Remote Access Configure	X				
Gateway Services: SSL VPN Configure	X				
Gateway Services: Static Routing Configure	X				
Gateway Services: BGP Routing View Only	X				
Gateway Services: DHCP View Only	X				
Gateway Services: Firewall View Only	X				
Gateway Services: IPSEC VPN View Only	X				
Gateway Services: L2 VPN View Only	X				
Gateway Services: Load Balancer View Only	X				
Gateway Services: NAT View Only	X				
Gateway Services: OSPF Rouing View Only	X				
Gateway Services: Remote Access View Only	X				
Gateway Services: SSL VPN View Only	X				
Gateway Services: Static Routing View Only	X				
Gateway Services: View Edge Gateway DNS	X	X	X	X	X
General: Administrator Control	X				
General: Administrator View	X				
General: Send Notification	X				
Hybrid Tunnel: Acquire Control Ticket	X				

Table 15-1. Rights Included in the Global Tenant Roles in vCloud Director (continued)

Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
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 the Cloud Tunnel Server Settings	X				
Hybrid Tunnel: View From-the-Cloud Tunnel	X				
Hybrid Tunnel: View To-the-Cloud Tunnel	X				
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				
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		

Table 15-1. 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: View vApp ACL	X	X	X	X	
Organization VDC: Edit Organization VDC Name and Description	X				
Organization VDC: Edit VM-VM Affinity Rule	X	X	X		
Organization VDC: Edit Organization VDC Extended Properties	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	X	
Organization VDC: View Organization VDC Extended Properties	X				
Organization VDC Network: View Properties	X				
Organization VDC Network: Edit Properties	X				
Organization VDC Network: Import Network	X				
Organization VDC: View Organization VDCs	X				
Organization VDC Template: Instantiate Organization VDC templates	X				
Organization VDC Template: View VDC templates	X				
Provider Network: View Provider Network	X				
Provider Network: Create / Delete Provider Network	X				
Role: Create / Update / Delete a Role	X				
SDDC: View SDDC	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 Group: View VDC Group	X				
VDC Group: Configure VDC Group	X				
VM Monitoring: View historic metrics for the Organization	X				
VM Monitoring: View historic metrics for the Organization VDC	X				

Table 15-1. 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: Access to VM Console	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			
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: Edit VM Compute Policy	X	X	X		
vApp: Manage VM Password Settings	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	

For information about the new rights that vCloud Director 10.0 introduces, see the *vCloud Director Service Provider Admin Portal Guide*.

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

16

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 SAML 2.0 compliant identity provider.
- Verify 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 a 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 15 Managing Users, Groups and Roles

Managing Your Organization 17

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**.

Working with Multiple Sites

The vCloud Director Multisite feature enables a service provider or a tenant of multiple, geographically-distributed vCloud Director installations (server groups) to manage and monitor those installations and their organizations as single entities.

The vCloud Director Tenant Portal provides **organization administrators** with a way to associate organizations at associated sites.

For more information about site associations, see the *vCloud Director Service Provider Admin Portal Guide*.

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 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 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 Service Library 18

The Service Library items in vCloud Director are vRealize Orchestrator workflows that extend the cloud management capabilities and make it possible for administrators of either providers or tenants to monitor and manipulate different services.

This chapter includes the following topics:

Search for a Service

The **Service Library** page in the vCloud Director Tenant Portal lists the set of vRealize Orchestrator workflows that are imported to vCloud Director and published to your organization.

Prerequisites

This operation requires the Service Library rights to be included in the predefined user role.

Procedure

1 From the main menu (☰), select **Libraries**, and under **Services** select **Service Library**.

The list of service items displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the service and a tag that corresponds to the service category where the vRealize Orchestrator is imported.

2 In the **Search** text box on the top of the page, enter the first word of either the name of the service or the name of the category, to which the service belongs.

a Select whether you want to search among the names of the service or among the categories.

The search results display in a card view of twelve items per page, sorted by names in alphabetical order.

Execute a Service

You can execute a service from the Service Library page in the vCloud Director Tenant Portal.

Prerequisites

This operation requires the Service Library rights to be included in the predefined user role.

Procedure

1. From the main menu (☰), select **Libraries**, and under **Services** select **Service Library**.

   The list of service items displays in a card view of 12 items per page, sorted by names in alphabetical order. Each card shows the name of the service and a tag that corresponds to the service category where the vRealize Orchestrator is imported.
2. Search for the service you want to execute.
3. Click **Execute** on the card of the service.

   A new dialog opens. You must enter values for the required input parameters of the service.
4. Click **Finish** to confirm the execution of the service.

What to do next

You can monitor the status of the execution in the **Recent Tasks** view. For more information, see View Tasks.

Working with Custom Entity Definitions

19

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.

Example

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.

The custom entity is removed from the card view.