VMware Cloud Director Service Provider Admin Guide

18 JUL 2023

VMware Cloud Director 10.5

vmware
by Broadcom

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

https://docs.vmware.com/

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

Contents

VMware Cloud Director™ Service Provider Admin Guide

1

This guide provides information about adding resources to VMware Cloud Director, managing and monitoring organizations, rights, roles, users, and groups in your cloud.

You can also create and manage NSX backed organization virtual data center networks.

Intended Audience

This guide is intended for service provider administrators who want to configure and manage a VMware Cloud Director installation. The information in this guide is written for experienced **system administrators**.

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 https://docs.vmware.com.

Getting Started with VMware Cloud Director Service Provider Admin Portal

2

The VMware Cloud Director Service Provider Admin Portal is a dedicated interface for service provider administrators.

Read the following topics next:

- Overview of VMware Cloud Director Administration
- Log in to VMware Cloud Director Service Provider Admin Portal
- Change the Language of the VMware Cloud Director UI by Using the VMware Cloud Director Service Provider Admin Portal
- Use the Quick Search in the VMware Cloud Director Service Provider Admin Portal
- View Tasks in Your VMware Cloud Director Service Provider Admin Portal
- Stop a Task in Progress in the VMware Cloud Director Service Provider Admin Portal
- View Events in the VMware Cloud Director Service Provider Admin Portal
- Set User Preferences in Your VMware Cloud Director Service Provider Admin Portal
- Length Limits on Names and Descriptions in Your VMware Cloud Director Service Provider Admin Portal
- Troubleshoot Failed Access to the VMware Cloud Director User Interface

Overview of VMware Cloud Director Administration

With VMware VMware Cloud Director you can build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual data centers and exposing them to users through Web-based portals and programmatic interfaces as a fully automated, catalog-based service.

The *VMware Cloud Director Service Provider Admin Guide* provides information about adding resources to the system, creating and provisioning organizations, managing resources and organizations, and monitoring the system.

vSphere and NSX Resources

VMware Cloud Director relies on vSphere resources to provide CPU and memory to run virtual machines. In addition, vSphere datastores provide storage for virtual machine files and other files necessary for virtual machine operations. VMware Cloud Director also uses vSphere distributed switches, vSphere port groups, and NSX Data Center for vSphere to support virtual machine networking.

VMware Cloud Director can also use resources from NSX. For information about registering an NSX Manager instance with your cloud, see the Register an NSX Manager Instance with VMware Cloud Director topic or the VMware Cloud Director API Programming Guide for Service Providers.

You can use the underlying vSphere and NSX resources to create cloud resources.

Starting with version 9.7, VMware Cloud Director can act as an HTTP proxy server, with which you can enable organizations to access the underlying vSphere environment.

Cloud Resources

Cloud resources are an abstraction of their underlying vSphere resources. They provide the compute and memory resources for VMware Cloud Director virtual machines and vApps. A vApp is a virtual system that contains one or more individual virtual machines with parameters that define operational details. Cloud resources also provide access to storage and network connectivity.

Cloud resources include provider and organization virtual data centers, external networks, organization virtual data center networks, and network pools.

Before you can add cloud resources to VMware Cloud Director, you must add vSphere resources.

Dedicated vCenter Server Instances and Proxies

A dedicated vCenter Server instance is a cloud resource that encapsulates an entire vCenter Server installation. A dedicated vCenter Server instance includes one or more proxies that are access points to different components of the underlying vSphere environment. The provider can create and enable dedicated vCenter Server instances and proxies. The provider can publish a dedicated vCenter Server instance to tenants.

To create and manage dedicated vCenter Server instances and proxies, you can use the Service Provider Admin Portal or the vCloud OpenAPI. See Chapter 9 Managing Dedicated vCenter Server Instances in VMware Cloud Director and Getting Started with VMware Cloud Director OpenAPI.

Provider Virtual Data Centers

A provider virtual data center combines the compute and memory resources of a single vCenter Server resource pool with the storage resources of one or more datastores available to that resource pool.

A provider virtual data center can use network resources from an NSX-V Manager instance that is associated with the vCenter Server instance or from an NSX Manager instance that is registered with the cloud.

You can create multiple provider virtual data centers for users in different geographic locations or business units, or for users with different performance requirements.

Organization Virtual Data Centers

An organization virtual data center provides resources to an organization and is partitioned from a provider virtual data center. Organization virtual data centers provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual media, such as floppy disks and CD ROMs.

A single organization can have multiple organization virtual data centers.

VMware Cloud Director Networking

VMware Cloud Director supports three types of networks.

- External networks
- Organization virtual data center networks
- vApp networks

Some organization virtual data center networks and all vApp networks are backed by network pools.

External Networks

An external network is a logical, differentiated network based on a vSphere port group. Organization virtual data center networks can connect to external networks to provide Internet connectivity to virtual machines inside a vApp.

Starting with version 9.5, VMware Cloud Director supports IPv6 external networks. An IPv6 external network supports both IPv4 and IPv6 subnets, and an IPv4 external network supports both IPv4 and IPv6 subnets.

By default, only **System Administrators** create and manage external networks.

Organization Virtual Data Center Networks

An organization virtual data center network belongs to a VMware Cloud Director organization virtual data center and is available to all the vApps in the organization. An organization virtual data center network allows vApps in an organization to communicate with each other. To provide external connectivity, you can connect an organization virtual data center network to an external network. You can also create an isolated organization virtual data center network that is internal to the organization.

VMware Cloud Director 9.5 introduces IPv6 support for direct and routed organization virtual data center networks.

Starting with VMware Cloud Director 9.5, **System Administrators** can create isolated virtual data center networks backed by an NSX logical switch. **Organization Administrators** can create isolated virtual data center networks backed by network pools.

VMware Cloud Director 9.5 also introduces cross-virtual data center networking by configuring stretched networks in virtual data center groups.

By default, only **System Administrators** can create direct and cross-virtual data center networks. **System Administrators** and **Organization Administrators** can manage organization virtual data center networks, although there are some limits to what an **Organization Administrators** can do.

vApp Networks

A vApp network belongs to a vApp and allows virtual machines in the vApp to communicate with each other. To enable a vApp to communicate with other vApps in the organization, you can connect the vApp network to an organization virtual data center network. If the organization virtual data center network is connected to an external network, the vApp can communicate with vApps from other organizations. vApp networks are backed by network pools.

Most users with access to a vApp can create and manage their own vApp networks. For information about working with networks in a vApp, see *VMware Cloud Director Tenant Guide*.

Network Pools

A network pool is a group of undifferentiated networks that is available for use within an organization virtual data center. A network pool is backed by vSphere network resources such as VLAN IDs or port groups. VMware Cloud Director uses network pools to create NAT-routed and internal organization virtual data center networks and all vApp networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Each organization virtual data center in VMware Cloud Director can have one network pool. Multiple organization virtual data centers can share one network pool. The network pool for an organization virtual data center provides the networks created to satisfy the network quota for an organization virtual data center.

Only **System Administrators** can create and manage network pools.

Organizations

VMware Cloud Director supports multi-tenancy by using 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. **Organization Administrators** tasks are described in *VMware Cloud Director Tenant Guide*.

Users and Groups

An organization can contain an arbitrary number of users and groups. **Organization Administrators** can create users, and import users and groups from a directory service such as LDAP. The **System Administrator** manages the set of rights available to each organization. The **System Administrator** can create and publish global tenant roles to one or more organizations. The **Organization Administrator** can create local roles in their organizations.

Catalogs

Organizations use catalogs to store vApp templates and media files. The members of an organization that have access to a catalog can use the containing vApp templates and media files to create their own vApps. A **System Administrator** can allow an organization to publish a catalog to make it available to other organizations. **Organization Administrators** can then decide which catalog items to provide to their users.

Log in to VMware Cloud Director Service Provider Admin Portal

You can access the VMware Cloud Director Service Provider Admin Portal by using a Web browser.

Prerequisites

You must have the system administrator rights to access the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 In a browser, type the Service Provider Admin Portal URL of your VMware Cloud Director site and press Enter.

   For example, type **`https://vcloud.example.com/provider`**.

2 Depending on your environment settings, choose one of the following.

   - To sign as a local user, enter the system administrator user name and password, and click **Sign In**.
   - To sign in using SSO, click **Sign In with Single Sign-On** and, if prompted, provide your credentials.

Change the Language of the VMware Cloud Director UI by Using the VMware Cloud Director Service Provider Admin Portal

The VMware Cloud Director user interface is available in English, German, French, Japanese, Korean, Simplified Chinese, Traditional Chinese, Italian, Spanish, and Brazilian Portuguese.

To change the language of the VMware Cloud Director UI, you must edit the language settings of the Web browser through which you are accessing the VMware Cloud Director UI.

Procedure

1. In the Web browser that you use to access the VMware Cloud Director UI, navigate to the language setting and change it to your preferred language.

   For example, if you are using Chrome, you must change the language of your Chrome browser.

2. Restart the browser.

Results

The VMware Cloud Director UI displays in your preferred language.

Use the Quick Search in the VMware Cloud Director Service Provider Admin Portal

You can use the VMware Cloud Director quick search to find screens, entities, and actions. The results depend on your location in the UI.

The results depend on the context, whether you selected an entity, and depending on the available actions for a particular entity. The search results are grouped into sections.

- Global Navigation - the results in this section are not related to a specific entity, for example, Edge Gateways, LDAP, Tasks, Trusted Certificates, Virtual Machines, and so on. You get these results regardless of where you are in the UI.
- Contextual Navigation - the results in this section depend on the selected entity in the UI. For example, vApp specific views like VMs, Network Diagram, and so on. If you select an entity like a vApp, the search shows both global and contextual navigation results and any actions that might be applicable to the entity.
- Contextual Actions - the results in this section depend on the selected entity in the UI. Depending on your location in the UI and the entity you select, by using the quick search results, you can perform an action related to the entity. For example, searching from the details view of a virtual machine displays results from the global views, contextual views, and actions that you can perform on the selected VM.
- Entity Search by Name - if you are viewing a list of entities, the search results can include also names of entities of the same type as the ones in the list. For example, if you are viewing a list of VMs, the search results include global navigation matches and matching names of VMs. If there is more than one page of entities in the list you are viewing, the search checks the full list of entities and might show a name that is not visible on the current page.

Procedure

1 Open the **Quick Search** window.

   - From the top navigation bar, click the **Help** menu and select **Quick Search**.
   - Press Ctrl+. or Cmd+., depending on your operating system.

2 Enter search criteria.

3 Browse through the results and select an option or perform an action by clicking or pressing Enter.

   You can use the up and down arrow keys to browse through the search results.

View Tasks in Your VMware Cloud Director Service Provider Admin Portal

From the Service Provider Admin Portal, you can view recent tasks and their status.

You can use the recent tasks view to monitor the status of tasks in your Service Provider Admin Portal. This view can be a good first step for troubleshooting any issues in your environment.

Next to the **Recent Tasks** button, the running and failed tasks appear in blue and red, respectively.

Procedure

1 In the lower-left corner, click **Recent Tasks**.

2 (Optional) Sort and filter the list of recent tasks.

Results

A lists of recent tasks displays, along with the status of the task, the type, the initiator, and the start and completion time.

Stop a Task in Progress in the VMware Cloud Director Service Provider Admin Portal

If you accidentally start a VMware Cloud Director™ 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**.

Results

The operation stops.

View Events in the VMware Cloud Director Service Provider Admin Portal

In the VMware Cloud Director UI, you can view the list of all events, 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. In the top navigation bar, click **Monitor** and **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.cloud*.
Organization	Name of the organization.

Detail	Description
Owner	User who triggered the event.
Time of occurrence	Date and time when the event occurred.

Set User Preferences in Your VMware Cloud Director Service Provider Admin Portal

You can set certain display and system alert preferences that take effect every time you log in to the system.

To learn more about leases, see Understanding Leases in VMware Cloud Director.

Procedure

1 In the top navigation bar, click your user name and select **User preferences**.

2 Select the page to appear when you log in.

  a Select the radio button next to **Start Page** and click **Edit**.

  b Select an option from the drop-down menu and click **Save**.

3 Configure an email notification for runtime lease expirations.

  a Select the radio button next to **Deployment Lease Alert Time** and click **Edit**.

  b Enter a value in seconds and click **Save**.

4 Configure an email notification for storage lease expirations.

  a Select the radio button next to **Storage Lease Alert Time** and click **Edit**.

  b Enter a value in seconds and click **Save**.

Length Limits on Names and Descriptions in Your VMware Cloud Director Service Provider Admin Portal

Follow these guidelines when entering values in VMware Cloud Director.

String values for the `name` attribute and the `Description` and `ComputerName` elements have length limitations that depend on the object to which they are attached.

Table 2-1. Length Limits on Object Properties

Object	Property	Maximum Length in Characters
`Catalog`	`name`	128
`Catalog`	`Description`	256
`EdgeGateway`	`name`	35
`Media`	`name`	128

Table 2-1. Length Limits on Object Properties (continued)

Object	Property	Maximum Length in Characters
`Media`	`Description`	256
`VApp`	`name`	128
`VApp`	`Description`	256
`VAppTemplate`	`name`	128
`VAppTemplate`	`Description`	256
`Vdc`	`name`	128
`Vdc`	`Description`	256
`Vm`	`name`	128
`Vm`	`ComputerName`	15 on Windows, 63 on all other platforms
`Vm`	`Description`	256

Troubleshoot Failed Access to the VMware Cloud Director User Interface

To view and update the valid IP addresses and DNS entries for the VMware Cloud Director cells in your VMware Cloud Director environment, you can use the VMware Cloud Director API.

Prerequisites

- Familiarize yourself with the relevant VMware Cloud Director API documentation.
- Verify that you have **system administrator** credentials.

Problem

You cannot access the VMware Cloud Director Service Provider Admin Portal or the VMware Cloud Director Tenant Portal after a successful login or after changing the DNS entries.

After you enter your credentials in the login screen, the following error message appears: `Failed to Start. An error was encountered during initialization. This can be caused by issues such as accessing the application via an unsupported public URL or poor connectivity.`

The access to the VMware Cloud Director UI might be limited even if the `Public Addresses` fields are properly configured.

For more information about the cause of the problem, see Configure CORS.

Solution

1. Make a `GET` request with an authorization header with the JSON Web Token (JWT) and an accept header to the `https://{api_host}/cloudapi/1.0.0/site/settings/cors` API endpoint.

   For more details and an alternative approach, see Configure CORS.

   The system output is a list that should contain HTTP and HTTPS entries with IP addresses and DNS names for all cells in the server group. It should also contain the public host name and IP address that the load balancer uses.

   Each endpoint in the list must have three entries:

   - FQDN
   - HTTP
   - HTTPS

   Example:

   ```
   {
     "values": [
        {
         "origin": "vcd.domain.local"
        },
        {
         "origin": "http://vcd.domain.local"
        },
        {
         "origin": "https://vcd.domain.local"
        }
      ]
   }
   ```

2. Verify that for every endpoint in the list, there are three entries and make a PUT request to the API endpoint.

   Verify that when you perform a REST PUT operation, you provide all values of the origins configuration which are currently configured and which you need to retain.

Managing Infrastructure Resources in VMware Cloud Director

3

VMware Cloud Director derives its resources from an underlying virtual infrastructure. After you register vSphere resources in VMware Cloud Director, you can allocate these resources for organizations to use.

VMware Cloud Director uses one or more vCenter Server environments to back its virtual data centers.

VMware Cloud Director can also use a vCenter Server environment to encapsulate an SDDC with one or more proxies. You can enable tenants to use these proxies as access points to the underlying vSphere environment from VMware Cloud Director with their VMware Cloud Director accounts.

Before you can use a vCenter Server instance in VMware Cloud Director, you must attach this vCenter Server instance.

Note VMware recommends that VMware Cloud Director manages a vCenter Server instance exclusively. When you use a vCenter Server instance for VMware Cloud Director and other purposes, a vCenter Server administrator might accidentally move VMware Cloud Director resources. This can cause VMware Cloud Director to operate incorrectly, including losing virtual machines that VMware Cloud Director manages.

When you create a provider virtual data center backed by an attached vCenter Server instance, this vCenter Server instance appears as published to a service provider, also called provider scoped. For information about creating a provider virtual data center, see Create a Provider Virtual Data Center in Your VMware Cloud Director.

When you create an SDDC that encapsulates an attached vCenter Server instance, you dedicated the vCenter Server to a tenant. This vCenter Server instance appears as published to a tenant, also called tenant scoped. For information about creating an SDDC, see Chapter 9 Managing Dedicated vCenter Server Instances in VMware Cloud Director.

Note By default, with an attached vCenter Server instance, you can create either a provider VDC or a dedicated vCenter Server instance. If you created a provider VDC backed by an vCenter Server instance, you cannot use this vCenter Server instance to create a dedicated vCenter Server instance, and the reverse.

Centralized SSL Management

Starting with version 10.1, VMware Cloud Director is moving to a centralized, tenant-aware storage area for certificate management. This way, VMware Cloud Director centralizes all certificates in one place so that **system administrators** and **organization administrators** can view, audit, and manage all certificates in use by various components in the system. You can use the VMware Cloud Director API to add, update, or remove certificates from the new tenant-aware storage area. See *VMware Cloud Director API Schema Reference*.

When adding or editing a new vCenter Server instance, NSX-V Manager instance, or NSX Manager instance, the VMware Cloud Director UI probes that endpoint for any certificates it is presenting. VMware Cloud Director adds to a centralized certificate storage area any certificate you decide to trust.

Managing Networking Resources

See Managing Network Infrastructure Resources in the VMware Cloud Director Service Provider Admin Portal.

Read the following topics next:

- Adding vCenter Server and NSX Data Center for vSphere Resources to VMware Cloud Director
- Accessing vSphere Components Through VMware Cloud Director Endpoints and Proxies
- View the vCenter Server Instances in Your VMware Cloud Director
- Modify vCenter Server Settings in Your VMware Cloud Director
- Activate or Deactivate a vCenter Server Instance in Your VMware Cloud Director
- Reconnect a vCenter Server Instance to Your VMware Cloud Director
- Refresh a vCenter Server Instance in Your VMware Cloud Director
- Managing Stranded Items in Your VMware Cloud Director
- Refresh the Storage Policies of a vCenter Server Instance in Your VMware Cloud Director
- Unregister a vCenter Server Instance From Your VMware Cloud Director
- Configuring and Managing Multisite Deployments in Your VMware Cloud Director
- Multisite Resource Lists in Your VMware Cloud Director
- Create a Site Association in Your VMware Cloud Director

Adding vCenter Server and NSX Data Center for vSphere Resources to VMware Cloud Director

You can use vSphere in combination with NSX Data Center for vSphere to provide CPU, memory, and storage to run virtual machines on VMware Cloud Director.

VMware Cloud Director can act as an HTTP server between tenants and the underlying vSphere environment.

For information about VMware Cloud Director system requirements and supported versions of vCenter Server and ESXi, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director

You can attach a vCenter Server instance so that its resources become available for use in VMware Cloud Director. You can attach a vCenter Server instance together with its associated NSX-V Manager instance.

For dedicated vCenter Server instances or for those associated with an NSX Manager instance, you can attach a vCenter Server instance alone.

VMware Cloud Director can use a vCenter Server instance either with its associated NSX-V Manager instance or with an NSX Manager instance.

If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must attach the vCenter Server and NSX-V Manager instances together.

If you want VMware Cloud Director to use this vCenter Server instance with an NSX Manager instance, you must attach the vCenter Server instance alone. After you attach the vCenter Server instance alone, you must Register an NSX Manager Instance with VMware Cloud Director.

Note After you attach a vCenter Server instance alone, you cannot add its associated NSX-V Manager instance at a later stage. You can unregister and attach again the vCenter Server instance together with its associated NSX-V Manager instance.

You can attach a vCenter Server instance to any site from your VMware Cloud Director environment.

You can attach a directly accessible vCenter Server instance or attach a vCenter Server instance that is behind a proxy. By using VMware Cloud Director OpenAPI, you can use proxy configurations within VMware Cloud Director to create a proxied connection between a VMware Cloud Director instance and the vCenter Server instance added to it. This way, the VMware Cloud Director and vCenter Server instances can exist in different locations or sites.

To attach a vCenter Server instance that is behind a proxy, first, you must declare a proxy configuration. Then, you must attach a vCenter Server instance, and configure VMware Cloud Director to use the proxy configuration when accessing the vCenter Server instance. You can also attach an NSX solution through a proxy. VMware Cloud Director does not support proxy configurations for NSX Data Center for vSphere. You do not need additional SSL configurations or an additional proxy configuration for the Platform Services Controller the vCenter Server instance is registered with.

Note In a configuration with a proxy, the VMware Cloud Director to proxy communication can use only HTTP. VMware Cloud Director does not support HTTPS proxy configurations. The communication with the vCenter Server instance, tunneled through the proxy, is HTTPS and uses the vCenter Server certificates.

Prerequisites

- If you configured VMware Cloud Director to verify vCenter Server and vSphere SSO certificates, test the connection to the vCenter Server instance and establish a trust relationship. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal..
- If you configured VMware Cloud Director to verify NSX-V Manager or NSX Manager certificates, test the connection to the NSX-V Manager or NSX Manager instance and establish a trust relationship. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal.

Procedure

1. Add the vCenter Server Instance to VMware Cloud Director

   To add a vCenter Server instance toVMware Cloud Director, you must enter the vCenter Server access details.

2. (Optional) Add the Associated NSX Manager Instance to VMware Cloud Director

   If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must add NSX-V Manager access details.

Add the vCenter Server Instance to VMware Cloud Director

To add a vCenter Server instance toVMware Cloud Director, you must enter the vCenter Server access details.

Prerequisites

Familiarize yourself with the vSphere certificate management options. See the vSphere Certificate Management Overview and Certificate Replacement Overview documentation. The VMware Cloud Director certificate strategy depends on your vSphere certificate choices.

vSphere Option	VMware Cloud Director Action
`Using VMCA-signed certificates`	In VMware Cloud Director, trust the CA certificate.
`Using the VMCA certificate as an intermediate certificate`	In VMware Cloud Director, trust the intermediate VMware Certificate Authority (VMCA) certificate.
`Using custom certificates where VMCA is not an intermediate certificate`	Trust the appropriate certificate so that VMware Cloud Director trusts all vSphere components like vCenter Server and ESXi. **Note** You must ensure that VMware Cloud Director trusts all necessary trust anchors.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **vCenter Server Instances** and click **Add**.

3 If you have a multisite VMware Cloud Director deployment, from the **Site** drop-don menu, select the site to which you want to add this vCenter Server instance, and click **Next**.

4 Enter a name and, optionally, a description for the vCenter Server instance in VMware Cloud Director.

5 Enter the URL of the vCenter Server instance.

If the default port is used, you can skip the port number. If a custom port is used, include the port number.

For example, **`https://`*`FQDN_or_IP_address`*`:`*`<custom_port_number>`***.

6 Enter the user name and password of the vCenter Server **administrator** account.

7 (Optional) To deactivate the vCenter Server instance after the registration, turn off the **Enabled** toggle.

8 Click **Next**.

9 If you haven't already established a trust relationship to the endpoint, on the **Trust Certificate** window confirm if you trust the endpoint.

Option	Description
Trust the connectivity to an endpoint when VMCA is in use	Use this option when in vSphere you are using VMCA-signed certificates or the VMCA as an intermediate certificate. a Review the initial certificate. b If VMCA is not included in the list of certificates, retrieve the additional CA certificates and, depending on your vCenter Server version, select one of the options. ■ For vCenter Server 7.0 and later, to fetch the additional CA certificates, click **Retrieve**. Select the VMCA certificate authority from the updated certificate chain, and trust it. ■ For vCenter Server 6.7 and earlier, you must manually retrieve the CA certificate from vSphere, and use the `Import` option to upload the certificate into the VMware Cloud Director certificates.
Trust the connectivity to an endpoint when VMCA is not in use	Use this option when in vSphere you are using custom certificates where VMCA is not an intermediate certificate a Review the initial certificate. b Determine the trust anchor to trust so that the entire vSphere infrastructure is trusted. Depending on your deployment, you might have to trust additional CAs. You must ensure that VMware Cloud Director trusts all necessary trust anchors. If necessary, use the `Trust Remote Connection` option.
Do not trust the connectivity to this endpoint	a Click **Cancel**. b Repeat Step 5 to Step 8 with a trusted endpoint.

10 (Optional) Skip adding the NSX-V Manager instance that is associated with the vCenter Server instance by turning off the **Configure Settings** toggle and click **Next**.

If you want VMware Cloud Director to use this vCenter Server instance with an NSX-V Manager instance, you must add the vCenter Server instance alone.

Note You cannot add the associated NSX-V Manager instance at a later stage. You can unregister and attach again the vCenter Server instance together with its associated NSX-V Manager instance.

11 If you want to add a tenant dedicated vCenter Server that will not be used as a provider VDC, turn on the **Enable tenant access** toggle.

After you add the vCenter Server instance to VMware Cloud Director, the tenant-related information appears in the details view of the instance.

12 If you want VMware Cloud Director to generate default proxies for the vCenter Server instance and SSO services, turn on the **Generate proxies** toggle.

After you add the vCenter Server instance to VMware Cloud Director, the proxies appear in the **Proxies** tab under **vSphere Resources**.

13 On the **Ready to Complete** page, review the registration details and click **Finish**.

14 If you haven't already trusted the necessary certificates, on the **Trust vSphere Certificate Authority** window, confirm that you trust the certificate so that VMware Cloud Director trusts all vSphere components and the integration with vSphere is complete.

   Important If you do not trust the vSphere CA, some VMware Cloud Director features do not work.

   You can trust the vSphere CA also after editing the vCenter Server instance.

What to do next

To enable operations acrossvCenter Server instances where the source and destination vCenter Server instances are not the same, verify that the vCenter Server instances trust each other independently of VMware Cloud Director. To view the certificates that a vCenter Server instance trusts, see the Explore Certificate Stores Using the vSphere Client in the *VMware vSphere Product Documentation*. Verify that each vCenter Server instance trusts the other vCenter Server instances that it needs to interact with. See also KB 89906.

(Optional) Add the Associated NSX Manager Instance to VMware Cloud Director

If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must add NSX-V Manager access details.

Procedure

1 On the **NSX-V Manager** page, leave the **Configure Settings** toggle turned on.

2 Enter the URL of the NSX-V Manager instance.

   If the default port is used, you can skip the port number. If a custom port is used, include the port number

   For example, **`https://`*`FQDN_or_IP_address`*`:`*`<custom_port_number>`***.

3 Enter the user name and password of the NSX **administrator** account.

4 (Optional) To enable cross-virtual data center networking for the virtual data centers backed by this vCenter Server instance, turn on the **Cross-VDC networking** toggle, and enter the control VM deployment properties and a name for the network provider scope.

   The control VM deployment properties are used for deploying an appliance on the NSX-V Manager instance for cross-virtual data center networking components like a universal router.

Option	Description
Network Provider Scope	Corresponds to the network fault domain in the network topologies of the data center groups. For example, **`boston-fault1`**. For information about managing cross-virtual data center groups, see the *VMware Cloud Director Tenant Guide*.
Resource Pool Path	The hierarchical path to a specific resource pool in the vCenter Server instance, starting from the cluster, *Cluster/Resource_Pool_Parent/ Target_Resource* . For example, **`TestbedCluster1/mgmt-rp`**. As an alternative, you can enter the Managed Object Reference ID of the resource pool. For example, **`resgroup-1476`**.
Datastore Name	The name of the datastore to host the appliance files. For example, **`shared-disk-1`**.
Management Interface	The name of the network in vCenter Server or port group used for the HA DLR management interface. For example, **`TestbedPG1`**.

5 Click **Next**.

6 If the endpoint does not have a trusted certificate, on the **Trust Certificate** window confirm if you trust the endpoint.

   - To add the endpoint to the centralized certificate storage area and continue, click **Trust** .
   - If you do not trust this endpoint, click **Cancel** and repeat Step 2 to Step 4 with a trusted endpoint.

7 Activate or deactivate the access configuration settings.

8 On the **Ready to Complete** page, review the registration details and click **Finish**.

What to do next

- Assign the NSX License Key in vCenter Server.
- Create a Provider Virtual Data Center in Your VMware Cloud Director.

Discovering and Adopting VMs in VMware Cloud Director

In the default configuration, a VMware Cloud Director organization VDC discovers virtual machines (VMs) that are created in any vCenter Server resource pool that backs the VDC.

After the **system administrator** grants you access to a discovered VM, you can reference the VM when you compose or recompose a vApp.

Each discovered VM is given a name that is derived from the name of the vCenter Server VM and a prefix specified by your organization administrator.

If you want to discover additional VMs, a **system administrator** can use the VMware Cloud Director API to create organization VDCs that adopt specified resource pools available from a provider VDC. vCenter Server VMs in these adopted resource pools appear in the new VDC as discovered VMs, and are candidates for adoption.

Note Virtual machines with IDE hard drives are discovered only if they are in powered off state.

If one or more vCenter VMs are not discovered by VMware Cloud Director, you can investigate the possible reasons by debugging the vCenter VM Discovery. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Activating VM Discovery

VM discovery is active by default. You can control VM discovery at three levels.

- Global setting at the cell level that **system administrators** can modify by using the Service Provider Admin Portal.

  a From the top navigation bar, select **Administration**.

  b In the left panel, under **Settings**, select **General**.

  c Edit the **Other** section.

  d Toggle the **VM discovery enabled** option.

  If the global-level setting is deactivated, then VM discovery is deactivated, regardless of the organization-level or VDC-level setting. If you want to override the global-level settings, see Activating VM Discovery by Using the VMware Cloud Director API section.

- Organization-level setting that **system administrators** can modify.

  a From the top navigation bar, select **Resources**.

  b In the left panel click **Organizations** and select the organization for which you want to modify the setting.

  c Under **Configure**, select **General**, and click to edit the **Other** section.

  d Select the VM discovery option for all VDCs in the organization.

  If the organization-level setting is deactivated, then VM discovery is deactivated on all VDCs in the organization, regardless of the VDC-level setting. If you want to override the organization-level settings, see Activating VM Discovery by Using the VMware Cloud Director API section.

- VDC-level setting that **system administrators** can modify.

  a From the top navigation bar, select **Resources**.

  b In the left panel click **Organization VDCs** and select the VDC for which you want to modify the setting.

  c Select the **General** tab and click **Edit** to modify the **Other** section.

  d Select the VM discovery option for the VDC.

Activating VM Discovery by Using the VMware Cloud Director API

VM discovery is active by default. To deactivate VM discovery for all organizations, a system administrator must update the value of the VmDiscoveryEnabled setting in the system's GeneralSettings. To deactivate VM discovery for all VDCs in an organization, an organization administrator must update the value of the VmDiscoveryEnabled setting in the GeneralOrgSettings for that organization. To deactivate VM discovery for an individual organization VDC, an organization administrator must update the value of the VmDiscoveryEnabled setting in the AdminVdc that represents the organization VDC.

To override the VM discovery default behavior, use the VMware Cloud Director API /api/admin/extension/settings/general to set the AllowOverrideOfVmDiscoveryByOrgAndOVDC parameter to true. When you set the parameter to true, you can modify the VM discovery settings at the organization and organization VDC level even if VM discovery is deactivated at the global level.

```
allow-override-of-vm-discovery-by-org-and-orgvdc = true
```

The AllowOverrideOfVmDiscoveryByOrgAndOVDC parameter is set to null by default and the global settings override all lower-level settings.

Using a VM from a Discovered VM

After the system administrator grants you access, you can use a discovered VM in the same ways you can use any other VM. For example, you can specify it when you build a new vApp. You can also clone a discovered VM or modify its name, description, or lease settings without triggering the adoption process.

Adopting a Discovered VM

You can adopt a discovered VM by changing its VM network. After you adopt a discovered VM, the system imports it and treats it as though it was created in VMware Cloud Director. When you retrieve an adopted VM with a VMware Cloud Director API request, the VM includes an element named autoNature. If the discovered VM was adopted or created in VMware Cloud Director, this element has a value of false . You cannot revert an adopted VM to a discovered VM.

Note Adopting a VM does not retain the VM reservation, limit, and shares settings that are configured in vCenter Server. Imported VMs obtain their resource allocation settings from the organization virtual data center (VDC) on which they reside.

Assign the NSX License Key in vCenter Server

If you attached a vCenter Server instance to its associated NSX-V Manager instance, you must assign a license key for the NSX-V Manager instance that supports VMware Cloud Director networking.

Prerequisites

Verify that you are logged in as a **system administrator**.

Procedure

1 From a vSphere Client that is connected to the vCenter Server system, select **Home > Licensing**.

2 For the report view, select **Asset**.

3 Right-click the NSX Manager asset and select **Change license key**.

4 Select **Assign a new license key** and click **Enter Key**.

5 Enter the license key, enter an optional label for the key, and click **OK**.

  Use the NSX Manager license key you received when you purchased VMware Cloud Director. You can use this license key in multiple vCenter Server instances.

6 Click **OK**.

Accessing vSphere Components Through VMware Cloud Director Endpoints and Proxies

You can use VMware Cloud Director endpoints to access the underlying vSphere environment. When endpoints are connected to proxies, VMware Cloud Director acts as an HTTP proxy server.

Endpoints

A VMware Cloud Director endpoint is an access point to a data center component, for example, a vCenter Server instance, an ESXi host, or an NSX-V Manager instance. Users can log in to the UI or API of proxied or non-proxied components by using their VMware Cloud Director accounts.

Creating a dedicated vCenter Server instance also creates a default endpoint for it. While attaching the vCenter Server instance, you can also create a proxy. However, the default endpoint is not connected to any proxy by default. You must edit the default endpoint or create a new one to connect it to a proxy.

You can create, edit, and delete endpoints from the **Endpoints** tab of a dedicated vCenter Server instance. See Create an Endpoint in VMware Cloud Director.

Proxies

The VMware Cloud Director provided proxies are different from the proxy configurations within VMware Cloud Director. Unlike VMware Cloud Director provided proxies that are scoped to a tenant, proxy configurations within VMware Cloud Director are on the provider level and there is no tenancy.

By activating and deactivating a VMware Cloud Director provided proxy, you can allow and stop the tenant access through that proxy.

You can create a proxy either when you attach a vCenter Server instance to VMware Cloud Director or later. If you create a proxy while attaching a vCenter Server and activating the tenant access, you must manually connect the proxy to the default endpoint.

If the vCenter Server instance uses an external Platform Services Controller, VMware Cloud Director creates a proxy for the Platform Services Controller as well. With parent and child proxies, you can hide certain proxies from the tenants or you can activate and deactivate groups of child proxies through their parent proxies. For information on creating a proxy after you add a vCenter Server instance to VMware Cloud Director, see Add a VMware Cloud Director Proxy for Accessing the Underlying vCenter Server Resources.

You can edit, activate, deactivate, and delete proxies from the **Proxies** tab under **Infrastructure Resources**.

Note When you add a proxy to a vCenter Server instance, you must upload the certificate and the thumbprint, so that tenants can retrieve the certificate and the thumbprint if the proxied component uses self-signed certificates.

To view and manage certificates and certificate revocation lists (CRLs), see Manage the Proxy Certificates and CRLs in VMware Cloud Director.

Create an Endpoint in VMware Cloud Director

In VMware Cloud Director, you can create endpoints that administrators and tenants can use to access the underlying vSphere environment.

Endpoints must be attached to dedicated vCenter Server instances and are visible to the tenants from the **Actions** menu of the dedicated vCenter Server instances. If you enable the tenant access when you add a vCenter Server instance to VMware Cloud Director, VMware Cloud Director creates a default endpoint with the vCenter Server instance URL as a target URL. If you create additional endpoints, you can change the default one.

Endpoints can serve as links between dedicated vCenter Server instances and proxies. Endpoints can have a connection to one proxy or they might not have a proxy connection. If an endpoint is connected to a proxy, the target of the endpoint is the target URL, not the UI URL of the connected proxy.

Prerequisites

Verify that the vCenter Server instance for which you want to create endpoints has enabled tenant access. See Enable the Tenant Access of an Attached vCenter Server in VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Select a vCenter Server instance.
4. On the page with detailed vCenter Server information, click the **Endpoints** tab and click **New**.
5. Enter a name and a target URL for the endpoint.
6. (Optional) Make this endpoint the default endpoint for this vCenter Server instance.

7 (Optional) Make a connection to a proxy.

8 Click **Save**.

What to do next

- Edit the endpoint settings.
- Delete an endpoint. If you want to delete the default endpoint, you must select another one as the default.

Add a VMware Cloud Director Proxy for Accessing the Underlying vCenter Server Resources

If you want VMware Cloud Director to act as an HTTP proxy server for vCenter Server instances and their components, you can create a proxy.

You can create proxies for dedicated vCenter Server instances and the vCenter Server instances that do not have a set purpose.

If you want to generate automatically a vCenter Server proxy with retrieved certificates and thumbprint, you can do so from the **vCenter Server Instances** grid or the vCenter Server details view. If the vCenter Server is with an external Platform Services Controller, this option also creates a proxy for the SSO endpoint.

This procedure describes how to create manually a proxy for a vCenter Server instance, or create a proxy for an ESXi host, external Platform Services Controller instance, or NSX-V Manager instance.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left panel, select **vCenter Server Instances**.

3 Select a vCenter Server instance.

4 On the page with detailed vCenter Server information, click the **Proxies** tab and click **New**.

5 Enter a name for the proxy.

6 Select the type of the proxy, depending on the component that you want VMware Cloud Director to be a proxy for.

   You cannot edit this setting after the creation of the proxy.

   You can create only one vCenter Server proxy. If there is an existing vCenter Server proxy and you want to create a new proxy, the **Type** drop-down menu does not include a vCenter Server option.

   - If you want to create a vCenter Server proxy, select **vCenter** from the **Type** drop-down menu and continue to Step 10.
   - If you want to create a proxy for an ESXi host, NSX-V Manager, or SSO, make your selection from the drop-down menu and continue to Step 7.

7 Enter a name, target host, and the UI URL of the new proxy.

   The target host is the host name or IP address of the component that you want VMware Cloud Director to be a proxy for. The UI URL of the new proxy is the URL to which the VMware Cloud Director UI directs to when the tenant opens the proxy.

8 If you want the proxy to be visible to the tenants, toggle on the **Tenant visible** option.

9 (Optional) Click **Select a parent proxy** and select a proxy from the list.

10 Click **Save**.

What to do next

Manage the Proxy Certificates and CRLs in VMware Cloud Director.

Manage the Proxy Certificates and CRLs in VMware Cloud Director

In VMware Cloud Director, you can view, download, and upload the proxy certificates and certificate revocation lists (CRLs).

Prerequisites

Verify that you have VMware Cloud Director provided proxies for at least one vCenter Server instance. See Accessing vSphere Components Through VMware Cloud Director Endpoints and Proxies.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left panel, click **Proxies**, and select a proxy.

3 Click **Manage Certificate**.

4 Upload or download the certificate and CRL.

5 Click **Save**.

View the vCenter Server Instances in Your VMware Cloud Director

You can see a list of the vCenter Server instances across all sites in your VMware Cloud Director installation. You can see how VMware Cloud Director uses each vCenter Server instance.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left panel, select **vCenter Server Instances**.

Results

A list of all attached vCenter Server instances is displayed. The list contains the following information for each vCenter Server instance.

	Description
Name	The name of the vCenter Server instance in VMware Cloud Director.
Status	The vCenter Server status can be normal, warning, and critical.
State	Activated or deactivated. See Activate or Deactivate a vCenter Server Instance in Your VMware Cloud Director.
Connection	Connected or not to VMware Cloud Director. See Reconnect a vCenter Server Instance to Your VMware Cloud Director.
VC Host	FQDN of the vCenter Server instance.
Version	The vCenter Server version.
Usage	Dedicated vCenter Server instances have enabled tenant access. The provider can use different resource pools of a shared vCenter Server instance across multiple provider VDCs and then allocate those resource pools to different tenants. See Chapter 9 Managing Dedicated vCenter Server Instances in VMware Cloud Director.
Cluster Health	Aggregation of the health of all clusters in the vCenter Server instance. When aggregating the heath of the cluster, the health of the least healthy cluster is displayed.
Clusters	Number of clusters in the vCenter Server instance.
VMs	Number of VMs in the vCenter Server instance.
Running VMs	Number of running VMs in the vCenter Server instance.
CPU	Amount of actively used virtual CPU as a percentage of the total available vCenter Server CPU.
Memory	Amount of actively used virtual memory as a percentage of the total available vCenter Server memory.
Storage	Amount of actively used virtual storage as a percentage of the total available vCenter Server storage.

Modify vCenter Server Settings in Your VMware Cloud Director

If the connection information for an attached vCenter Server instance changes, or if you want to change its name and description in VMware Cloud Director, or its compute provider scope, you can edit the vCenter Server settings.

You can edit the settings that you configured when adding the vCenter Server instance. See Add the vCenter Server Instance to VMware Cloud Director.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **vCenter Server Instances** and click the name of the vCenter Server instance that you want to modify.

3 In the upper-right corner of the **vCenter Server Info** section, click **Edit**.

4 (Optional) Edit the name and description of the instance.

5 (Optional) Edit the compute provider scope for the vCenter Server

   The compute provider scope represents compute fault domains, or availability zones which are visible to tenants and where workloads reside. By default, the compute provider scope of a provider virtual data center is inherited from the backing vCenter Server instance. You can differentiate the compute provider scope for the different provider VDCs that are backed by a single vCenter Server instance. For example, you can set the vCenter Server with a compute provider scope **`Germany`** and you can set the provider VDC with a scope **`Munich`**.

6 (Optional) Edit the URL for the vCenter Server instance.

7 (Optional) Edit the user name and password for the vCenter Server **administrator** account.

8 (Optional) Turn on or off the **Enabled** toggle.

9 Click **Save**.

10 If you haven't already trusted the necessary certificates, on the **Trust vSphere Certificate Authority** window, confirm that you trust the certificate so that VMware Cloud Director trusts all vSphere components and the integration with vSphere is complete.

   Important If you do not trust the vSphere CA, some VMware Cloud Director features do not work.

   The **Trust vSphere Certificate Authority** window appears after each edit of the vCenter Server instance until you import the necessary certificates.

What to do next

If you modified the connection information, you must Reconnect a vCenter Server Instance to Your VMware Cloud Director.

Activate or Deactivate a vCenter Server Instance in Your VMware Cloud Director

Before performing a maintenance or unregistering a vCenter Server instance, in VMware Cloud Director, you must deactivate the target vCenter Server instance.

To provide its resources to virtual data centers in VMware Cloud Director, you must activate the vCenter Server instance.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Click the radio button next to the name of the target vCenter Server instance, and click **Enable** or **Disable**.
4. To confirm, click **OK**.

Reconnect a vCenter Server Instance to Your VMware Cloud Director

If a vCenter Server instance appears as disconnected, or if you modified the connection settings, you can try to reset the connection to VMware Cloud Director.

Note During establishing the new connection, the vCenter Server instance is unavailable for operations.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Click the radio button next to the name of the target vCenter Server instance, and click **Reconnect**.
4. To confirm, click **OK**.

Refresh a vCenter Server Instance in Your VMware Cloud Director

To update the information in the VMware Cloud Director database about the underlying vCenter Server resources, you must refresh the vCenter Server instance.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Click the radio button next to the name of the target vCenter Server instance, and click **Refresh**.
4. To confirm, click **OK**.

Managing Stranded Items in Your VMware Cloud Director

When you delete an object in VMware Cloud Director and that object also exists in vSphere, VMware Cloud Director attempts to delete the object from vSphere. In some situations, VMware Cloud Director may not be able to delete the object in vSphere, in which case, the object becomes stranded.

You can view a list of stranded items and try again to delete them, or you can use the vSphere Client to delete the stranded objects in vSphere.

Delete a Stranded Item from Your VMware Cloud Director

You can delete a stranded item to try to remove an object from vSphere that you already deleted from VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Click **Stranded Items**.
3. Select the stranded item and click **Delete**.
4. (Optional) Select the **Force delete** check box.

   This removes the stranded item from the stranded items list, but the stranded item continues to exist in vSphere.
5. Click **Ok**.

Refresh the Storage Policies of a vCenter Server Instance in Your VMware Cloud Director

To update the information in the VMware Cloud Director database about the VM storage policies in the underlying vSphere environment, you must refresh the storage policies of the vCenter Server instance.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Click the radio button next to the name of the target vCenter Server instance, and click **Refresh Policies**.
4. To confirm, click **OK**.

Unregister a vCenter Server Instance From Your VMware Cloud Director

To stop using the resources of a vCenter Server instance, you can remove this vCenter Server instance from your VMware Cloud Director installation.

Prerequisites

- Deactivate the vCenter Server instance. See Activate or Deactivate a vCenter Server Instance in Your VMware Cloud Director.
- Delete all provider virtual data centers that use resource pools from this vCenter Server instance. See Delete a Provider Virtual Data Center in Your VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Click the radio button next to the name of the target vCenter Server instance, and click **Unregister**.
4. To confirm, click **OK**.

Configuring and Managing Multisite Deployments in Your VMware Cloud Director

To manage and monitor multiple, geographically distributed VMware Cloud Director installations or server groups and their organizations as single entities, you can use the VMware Cloud Director multisite feature.

Effective Implementation of a Multisite

When you associate two VMware Cloud Director sites, you enable the administration of the sites as a single entity. You also enable organizations at those sites to form associations with each other. See Create a Site Association in Your VMware Cloud Director. When an organization is a member of an association, organization users can use the VMware Cloud Director Tenant Portal to access organization assets at any member site, although each member organization and its assets are local to the site it occupies.

Note The sites must be with the same VMware Cloud Director API version, or one major version apart. For example, you can associate a VMware Cloud Director 10.1 (API version 34.0) site with a VMware Cloud Director site version 10.0, 10.1, 10.2 or 10.2.2, respectively API versions 33.0, 34.0, 35.0, or 35.2.

After you associate two sites, you can use the VMware Cloud Director API or the VMware Cloud Director Tenant Portal to associate organizations that occupy those sites. See the *VMware Cloud Director API Programming Guide* or the Configure and Manage Multisite Deployments topic in the *VMware Cloud Director Tenant Guide*.

A site or organization can form an unlimited number of associations with a peer, but each association includes exactly two members. Each site or organization must have its own private key. Association members establish a trust relationship by exchanging public keys, which are used to verify signed requests from one member to another.

Each site in an association is defined by the scope of a VMware Cloud Director server group (a group of servers that share a VMware Cloud Director database). Each organization in an association occupies a single site. The organization administrator controls access by organization users and groups to assets at each member site.

Site Objects and Site Associations

The installation or upgrade process creates a `Site` object that represents the local VMware Cloud Director server group. A system administrator whose authority extends to more than one VMware Cloud Director server group can configure those server groups as an association of VMware Cloud Director sites.

Site Names

Each `Site` object is created with a name attribute that is a UUID.

```
GET https://Site-B.example.com/api/site
...
<Site name="b5920690-fe13-4c31-8e23-9e86005e7a7b" ...>
   ...
   <RestEndpoint>https://Site-A.example.com/api/org/Org-A</RestEndpoint>
   <RestEndpointCertificate>-----BEGIN CERTIFICATE-----
```

```
      MIIDDTCCAfWgAwIBAgI...Ix0eSE= -----END CERTIFICATE-----
   </RestEndpointCertificate>
   ...
</Site>
```

While there is no requirement that the site name matches the hostname in the API endpoint, a system administrator can update the site name as an administrative convenience for VMware Cloud Director API users, with a request like this one:

```
PUT https://Site-B.example.com/api/site
content-type: application/vnd.vmware.vcloud.site+xml
...
<Site name="Site-B" ...>
   ...
   <RestEndpoint>https://Site-A.example.com/api/org/Org-A</RestEndpoint>
   <RestEndpointCertificate>-----BEGIN CERTIFICATE-----
      MIIDDTCCAfWgAwIBAgI...Ix0eSE= -----END CERTIFICATE-----
   </RestEndpointCertificate>
   ...
</Site>
```

The `Site` element in the request body must retain the formatting in which it was returned by the `GET .../site` request. Additional characters, particularly carriage-returns, line feeds, or spaces, before or after the certificates can cause the system to return a bad request exception.

Associations of Organizations

After site association is complete, **organization administrators** at any member site can begin associating their organizations.

Note You cannot associate a `System` organization with a tenant organization. The `System` organization at any site can be associated only with the `System` organization at another site.

Authorization Headers and Request Fanout

The `Session` response to a successful login request includes an `X-VMWARE-VCLOUD-ACCESS-TOKEN` header whose value is an encoded key that you can use, and the value of the `X-VMWARE-VCLOUD-TOKEN-TYPE` header, to construct a JWT `Authorization` header to include in subsequent requests in place of the deprecated `x-vcloud-authorization` header, which does not authenticate you to association members. See Create a VMware Cloud Director API Session for more information about logging in to the VMware Cloud Director API.

You can make requests that fan out to multiple association members by specifying the `multisite=`*value* pair in the `Accept` header. If you want the request to fan out, the *value* can be `global` or a colon-separated list of location IDs. For information about obtaining the location IDs, see Authorized Locations. When you set the *value* to `local`, the request does not fan out but includes multisite metadata included on fan-out.

For example, when you make a request such as a query that retrieves lists of resources from an association of organizations, you can specify the `multisite=global` pair in the `Accept` header. By specifying the `multisite=global` pair, you fan out the request to all association members and return an aggregated list.

```
Accept: application/*;version=30.0;multisite=global
```

You can specify a colon-separated list of location IDs, for example, `multisite=`*ID-a:ID-b:ID-x*. Unless you include this value in the `Accept` header, the request returns only those resources owned by the organization that is the target of the request. Unless you are making a request to the same organization that you authenticated to, you must also include a `X-VMWARE-VCLOUD-AUTH-CONTEXT` header that specifies the name of the organization that will fulfill your request.

When an authentication request includes the `multisite=`*value* pair, the response includes `Link` elements if the request failed at any association member. The category of the failure is represented by the `rel` value of the link.

`rel="fanout:failed"`

Member status was `ACTIVE` but authentication at the member failed for some other reason.

`rel="fanout:skipped"`

Authentication at the member was skipped because the association status was `ASYMMETRIC` or `UNREACHABLE`.

The failed or skipped request URL is in the `href` the value of the `Link`.

Authorized Locations

When you authenticate to a site that is a member of an association, the `Session` response includes an `AuthorizedLocations` element that provides VMware Cloud Director API and VMware Cloud Director Tenant Portal endpoints for other association members. In this example:

- `Site-A.example.com` and `Site-B.example.com` are associated.
- The user logs in to Site-A as a **system administrator**.

Request:

```
POST https://Site-A.example.com/api/sessions
Authorization: Basic ...
Accept: application/*;version=30.0
...
```

Response:

```
200 OK
...
X-VMWARE-VCLOUD-ACCESS-TOKEN: eyJhbGciOiJSUzI1NiJ9....Rn4Xw
X-VMWARE-VCLOUD-TOKEN-TYPE: Bearer
Content-Type: application/vnd.vmware.vcloud.session+xml;version=30.0;multisite=global
```

```
...
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Session ...
   ...
   <AuthorizedLocations>
      <Location>
         <LocationId>a93c9db9-7471-3192-8d09-a8f7eeda85f9@9a41...
         </LocationId>
         <SiteName>Site-A</SiteName>
         <OrgName>System</OrgName>
         <RestApiEndpoint>https://site-a.example.com
         </RestApiEndpoint>
         <UIEndpoint>https://site-a.example.com
         </UIEndpoint>
         <AuthContext>System</AuthContext>
      </Location>
      <Location>
         <LocationId>a93c9db9-7471-3192-8d09-a8f7eeda85f9@4f56...
         </LocationId>
         <SiteName>Site-B</SiteName>
         <OrgName>System</OrgName>
         <RestApiEndpoint>https://site-b.example.com
         </RestApiEndpoint>
         <UIEndpoint>https://site-b.example.com
         </UIEndpoint>
         <AuthContext>System</AuthContext>
      </Location>
   </AuthorizedLocations>
</Session>
```

User and Group Identities

Associations of sites and organizations must agree to use the same identity provider (IDP). User and group identities for all organizations in the association must be managed through this IDP.

Associations are free to choose the IDP that works best for them. See Managing Identity Providers in VMware Cloud Director.

Starting with VMware Cloud Director 10.4.1, service accounts can manage and monitor multiple, geographically distributed VMware Cloud Director installations or server groups and their organizations as single entities by using the multisite feature. If a service account is making a request to a different organization from the one that it is authenticated to, verify that the service account exists on the associated organization and that it has the same name and software ID. See Managing Service Accounts in VMware Cloud Director.

Site Access Control for Organization Users and Groups

Organization administrators can configure their IDP to generate user or group access tokens that are valid at all member sites, or valid at only a subset of member sites. While user and group identities must be the same in all member organizations, user and group rights are constrained by the roles those users and groups are assigned in each member organization. Assignment of a role to a user or group is local to a member organization, as are any custom roles you create.

Load Balancer Requirements

Effective implementation of a multisite deployment requires you to configure a load balancer that distributes requests arriving at an institutional endpoint such as `https://vcloud.example.com` to the endpoints for each member of the site association (for example, `https://us.vcloud.example.com` and `https://uk.vcloud.example.com`). If a site has more than one cell, you must also configure a load balancer that distributes incoming requests across all its cells, so that a request to `https://us.vcloud.example.com` can be handled by `https://cell1.us.vcloud.example.com`, `https://cell2.us.vcloud.example.com`, and so on.

Note You must use the global load balancer, in this case `https://vcloud.example.com`, only for UI access. If you develop your own scripts or programs that use the REST API, those calls must target a particular site.

Starting with VMware Cloud Director 10.3, all client requests that arrive at the load-balancing endpoint for a multisite deployment are redirected. When a request arrives at the load-balancing endpoint, even if the site where the request arrives is the correct one, a redirect is issued and reflected in the user-visible URL to specify that the request was directed to the correct location.

For example, you can have a deployment consisting of two sites - `https://site1.vcloud.example.com` and `https://site2.vcloud.example.com` - behind a global load-balancing endpoint `https://us.vcloud.example.com`. Starting with VMware Cloud Director 10.3, when a request arrives at the load-balancing endpoint for an organization that is located at site 1 - `https://us.vcloud.example.com/org1`, if the request lands at site 1, then site issues a redirect to itself by forwarding the request to `https://site1.vcloud.example.com/org1`. VMware Cloud Director 10.2.x and earlier versions do not issue redirects when a load balancer receives a request for an organization that is located at the same place and the request is serviced through the public endpoint's URL `https://us.vcloud.example.com/org1`.

Network Connectivity Requirements

If you want to use the multisite feature, each cell at each site must be able to make REST API requests to the REST API endpoints of all sites. If you use the examples from the Load Balancer Requirements section, `cell1.us.vcloud.example.com` and `cell2.us.vcloud.example.com` must be able to reach the REST API endpoint for `uk.example.com`. The reverse is true for all cells under `uk.example.com`. This means that a cell must also be able to make REST API calls to it's own REST API endpoint, so `cell1.us.vcloud.example.com` must be able to make a REST API call to `https://us.vcloud.example.com`.

Making REST API requests to the REST API endpoints of all sites is necessary for of REST API fanout. For example, if the UI or an API client makes a multisite request to get a page of organizations from all sites and `cell1.us.vcloud.example.com` handle the request. The cell `cell1` must make a REST API call to get a page of organizations from each site using the REST API endpoint configured for that site. When all sites return their page of organizations, `cell1` collates the results and returns a single page of results containing the data from all other sites.

Sites and Certificates

When a site is associated with other sites, if you update its certificate, you might have to let the other sites know of the change. If you do not let the other sites know about the certificate change, the multisite fanout might be impacted.

If you are replacing a certificate on a site with a valid, well-signed certificate, then you do not need to inform the other sites. Because the certificate is valid and well-signed, the cells at the other sites can continue connecting to it in a secure manner without interruption.

If you are replacing a certificate on a site with a self-signed certificate, or if there is some other problem with the certificate that prevents automatic trust, then other sites need to know. For example, if the certificate expires, you must let the other sites know. At each of the other sites, you must upload the certificate into the **Trusted Certificates** in the Service Provider Admin Portal. See Import Trusted Certificates Using Your VMware Cloud Director Service Provider Admin Portal. When you import the certificate, the site where the certificate is uploaded can trust the site getting the new certificate.

Note You can import these certificates to the Trusted Certificates of the other sites before you install them at the remote site. This ensures no interruptions in communication because both the old certificate and the new certificate are in the Trusted Certificates pool. You do not have to reassociate the sites.

Association Member Status

After you create an association of sites or organizations, the local system periodically retrieves the status of each remote association member and updates that status in the local site's VMware Cloud Director database.The member status is visible in the `Status` element of an `SiteAssociationMember` or `OrgAssociationMember`. The `Status` element can have one of three values:

`ACTIVE`

The association has been established by both parties, and communication with the remote party was successful.

`ASYMMETRIC`

The association has been established at the local site, but the remote site has not yet reciprocated.

`UNREACHABLE`

An association has been created by both parties, but the remote site is not currently reachable on the network.

In the Service Provider Admin Portal and Tenant Portal the statuses appear as `Connected`, `Partially Connected`, and `Unreachable`.

The member status "heartbeat" process runs with the identity of the multisite system user, a local VMware Cloud Director user account created in the System organization during VMware Cloud Director installation. Although this account is a member of the System organization, it does not have system administrator rights. It has only a single right, `Multisite: System Operations`, which gives it permission to make a VMware Cloud Director API request that retrieves the status of the remote member of a site association.

Multisite Resource Lists in Your VMware Cloud Director

If you are working with VMware Cloud Director deployments in multiple locations, you can view resource lists that include information about objects from all the connected sites.

To facilitate navigating through vSphere and cloud resources from the Service Provider Admin Portal, starting with version 9.7, VMware Cloud Director introduces multisite resource lists. Starting with version 10.0, VMware Cloud Director supports multisite resource lists that include organizations.

You can access the resource lists through the **vSphere Resources** and the **Cloud Resources** menus.

You can access detailed information about objects from the different sites and also create objects both on the local site and on remote sites.

Multisite vSphere resources lists are supported for vCenter Server instances, NSX Manager instances, resource pools, datastores, hosts, distributed switches, port groups, stranded items, and storage policies.

Multisite cloud resources lists are supported for organizations, organization VDCs, organization VDC templates, provider VDCs, cloud cells, edge gateways, external networks, network pools, and VM sizing policies.

Create a Site Association in Your VMware Cloud Director

You can associate sites to enable the administration of the sites as a single entity in VMware Cloud Director. You can also enable organizations at those sites to form associations with each other.

When an organization is a member of an association, organization users can use the VMware Cloud Director Tenant Portal to access organization assets at any member site, although each member organization and its assets are local to the site it occupies.

Prerequisites

Verify that the sites you want to associate are with the same VMware Cloud Director API version, or one major version apart. For example, you can associate a VMware Cloud Director 10.1 (API version 34.0) site with a VMware Cloud Director site version 10.0, 10.1, 10.2 or 10.2.2, respectively API versions 33.0, 34.0, 35.0, or 35.2.

Procedure

1 Retrieve the local association data of a site you want to associate.

  a Log in to the Service Provider Admin Portal of the site you want to associate.

  b From the top navigation bar, select **Administration**.

  c In the left panel, under **Settings**, click **Multisite**.

  d Click **Download Local Data**, and save the XML file.

2 Repeat Step 1a to Step 1d at each site you want to associate.

3 On any of the sites, click **New Site Association**.

4 Click **Upload**, select the data file from another site, and click **Open**.

5 To create the site association, click **Create** and select the relevant option for your site association configuration.

Option	Description
Create and Add Another	Select this option if you are associating more than two sites.
Create and Go to Associated Site	Select this option if you are associating two sites and want to go directly to the second site to upload the data file for the first.
Create and Close	Select this option if you want to complete the site association on this site and close the window. You must manually navigate to another site to upload the relevant data files.

When you upload the data file to only one of the sites, you create a partial connection. To complete the association, you must upload all respective data files to each associated site. For example, if you are associating Site-A, Site-B, and Site-C. On Site-A, you must upload the data files for Site-B and Site-C. On Site-B, you must upload the data files for Site-A and Site-C. On Site-C, you must upload the data files for Site-A and Site-B. When you upload all the necessary files, the sites become `Connected`.

6 If you want to associate more than two sites, upload the data files for the sites you want to associate.

   a Upload the data files for the sites you want to associate with this site.

   b Click **Create** and select **Create and Close**.

   c Navigate to the **Multisite** tab on each site you want to associate, and upload the data files of the other sites.

What to do next

- After you associate two sites, you can use the VMware Cloud Director API or the VMware Cloud Director Tenant Portal to associate organizations that occupy those sites. See the *VMware Cloud Director Tenant Guide*.
- To delete an association, on the card of the site, select **Actions > Delete**.

Managing Cloud Resources in Your VMware Cloud Director

4

Cloud resources are an abstraction of their underlying vSphere resources and provide the compute and memory resources for VMware Cloud Director virtual machines and vApps, and access to storage and network connectivity.

Cloud resources include cloud cells, provider and organization virtual data centers, external networks, organization virtual data center networks, and network pools. Before you can add cloud resources to VMware Cloud Director, you must add vSphere resources.

For information about organization virtual data centers, see Chapter 8 Managing Organization Virtual Data Centers in VMware Cloud Director.

For information about organization virtual data center networks, see the Managing Organization Virtual Data Center Networks chapter in the *VMware Cloud Director Tenant Guide*.

The SDDC or dedicated vCenter Server instance as a cloud resource in VMware Cloud Director encapsulates an entire vCenter Server installation. The provider can create and enable a dedicated vCenter Server, publish it to tenants, and create and enable proxies to different components of the underlying vSphere environment. To create, publish to tenants, and manage dedicated vCenter Server instances and proxies, you can use the Service Provider Admin Portal or VMware Cloud Director OpenAPI. See Chapter 9 Managing Dedicated vCenter Server Instances in VMware Cloud Director or Getting Started with VMware Cloud Director OpenAPI.

For information on managing networking resources, see Managing Cloud Networking Resources in the VMware Cloud Director Service Provider Admin Portal.

Read the following topics next:

- Provider Virtual Data Centers in Your VMware Cloud Director
- Create a Provider Virtual Data Center in Your VMware Cloud Director
- View and Manage Your VMware Cloud Director Cell Infrastructure

Provider Virtual Data Centers in Your VMware Cloud Director

In VMware Cloud Director, a provider virtual data center (VDC) combines the compute and memory resources of vCenter Server resource pools with the storage resources of one or more storage policies from a single vCenter Server instance.

For network resources, a provider VDC can use NSX Data Center for vSphere, NSX, or the networking resources of vSphere.

- You can create and manage a provider VDC backed by an attached vCenter Server instance and its associated NSX-V Manager instance by using the Service Provider Admin Portal or the vCloud API.
- You can create and manage a provider VDC backed by an attached vCenter Server instance and an NSX Manager instance by using the Service Provider Admin Portal or the vCloud API.
- If you plan to only use vSphere networking resources, you can create a provider VDC without a network pool.

A typical VMware Cloud Director system includes multiple provider VDCs configured to meet various service level requirements. Each provider VDC has a primary resource pool. You can add and remove non-primary resource pools from the backing vCenter Server instance. You cannot remove the primary resource pool.

Create a Provider Virtual Data Center in Your VMware Cloud Director

To make vSphere compute, memory, and storage resources available to VMware Cloud Director, you create a provider virtual data center (VDC).

Before an organization can begin deploying VMs or creating catalogs, the **system administrator** must create a provider VDC and the organization VDCs that consume its resources. The relationship of provider VDCs to the organization VDCs they support is an administrative decision. The decision can be based on the scope of your service offerings, the capacity and geographical distribution of your vSphere infrastructure, and similar considerations. Because a provider VDC constrains the vSphere capacity and services available to tenants, **system administrators** commonly create provider VDCs that furnish different classes of service, as measured by performance, capacity, and features. Tenants can then be provisioned with organization VDCs that deliver specific classes of service defined by the configuration of the backing provider VDC.

Before you create a provider VDC, consider the set of vSphere capabilities that you plan to offer your tenants. Some of these capabilities can be implemented in the primary resource pool of the provider VDC. Others might require you to create additional resource pools based on specially configured vSphere clusters and add them to the VDC as described in Add a Resource Pool to a VMware Cloud Director Provider Virtual Data Center.

The range of ESXi releases installed on hosts in the cluster backing a resource pool determines the set of guest operating systems and virtual hardware versions available to VMs deployed in organization VDCs backed by the provider VDC.

Prerequisites

- Log in to the Service Provider Admin Portal as a **system administrator**.

- Verify that you created the target primary resource pool with available capacity in a cluster configured to use automated DRS. You can use a resource pool for only one provider VDC. To create a resource pool, you can use the vSphere Client.
- If you plan to use a resource pool that is part of a cluster that uses vSphere High Availability (HA), verify that you are familiar with how vSphere HA calculates the slot size. For information about slot sizes and customizing vSphere HA behavior, see the *vSphere Availability* documentation.
- If you want to use vSphere with Tanzu in VMware Cloud Director, verify that you have available a vCenter Server 7.0 or later instance with a configured Supervisor Cluster. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation.
- If you want to use vSphere with Tanzu in VMware Cloud Director and you are using vCenter Server 7.0 Update 3 instance with a configured Supervisor Cluster, you must not configure no-NAT rules for the Supervisor Cluster namespaces.
- If you use NSX Data Center for vSphere for the network resources of the provider VDC:
  - Verify that the vCenter Server instance that contains the target primary resource pool is attached and has a NSX Data Center for vSphere license key.
  - Set up the VXLAN infrastructure in NSX Manager. See the relevant *NSX Administration Guide*.

    If you want to use a custom VXLAN network pool in this provider VDC instead of the default VXLAN network pool, create that network pool now. See Create a Network Pool Backed by an NSX Data Center for vSphere Transport Zone in Your VMware Cloud Director.
- If you use NSX for the network resources of the provider VDC:
  - Add a Provider Gateway to Your VMware Cloud Director
  - Create a Network Pool Backed by an NSX Transport Zone in Your VMware Cloud Director

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click **New**.
4. If you have a multisite VMware Cloud Director deployment, from the **Site** drop-don menu, select the site to which you want to add this provider VDC instance, and click **Next**.
5. Enter a name and, optionally, a description for the provider VDC.

   You can use these text boxes to indicate the vSphere features available to organization VDCs backed by this provider VDC, for example, **`vSphere HA`** or **`Storage policies with IOPS support.`**

6 (Optional) To deactivate the provider VDC upon creation, turn off the **State** toggle.

You cannot use the compute and storage resources of a deactivated VDC for the creation of organization VDCs.

7 Click **Next**.

8 To provide resource pools for the provider VDC, select a vCenter Server instance, and click **Next**.

This page lists vCenter Server instances registered to VMware Cloud Director. Clicking a vCenter Server instance shows its available resource pools.

If you want to use vSphere with Tanzu in VMware Cloud Director, you must select a vCenter Server 7.0 or later instance with a configured Supervisor Cluster.

9 Select a resource pool to serve as the primary resource pool for this provider VDC.

You can use one resource pool for one provider VDC. When you add a resource pool to a provider VDC, this resource pool and its parent chain become unavailable for selection for other provider VDCs.

If you want to use vSphere with Tanzu, select a Supervisor Cluster. VMware Cloud Director displays a Kubernetes icon next to resource pools backed by a Supervisor Cluster.

10 If you select a resource pool or cluster that is backed by a Supervisor Cluster, to establish a trust relationship with the Kubernetes control plane, you must trust the Kubernetes control plane certificate.

11 Select the highest virtual hardware version you want the provider VDC to support, and click **Next**.

The system determines the highest virtual hardware version supported by all hosts in the cluster that backs the resource pool and offers it as the default in the **Highest supported hardware version** drop-down menu. You can use this default or select a lower hardware version from the menu. The version you specify becomes the highest virtual hardware version available to a VM deployed in an organization VDC backed by this provider VDC. If you select a lower virtual hardware version, some guest operating systems might not be supported for use by those VMs. Once you create the provider VDC with the selected hardware version, you can only upgrade the version, you cannot downgrade it.

The available hardware version for the provider VDC depends on the highest available version of the ESXi host in the target cluster. If the highest supported hardware version of the ESXi host is not available for selection, verify in the vSphere Client that the default compatibility for virtual machine creation on the data center is set to **`Use datacenter setting and host version`**. You can also set the default compatibility setting to the highest hardware version you want for the cluster.

VMware Cloud Director 9.7 and later support the highest hardware version that the backing vSphere infrastructure supports. Starting with VMware Cloud Director 10.2.2, you can set the hardware version without manually configuring the default hardware version in the vCenter Server instance.

12 Select one or more storage policies for the provider VDC, and click **Next**.

All vSphere storage policies supported by the resource pool you selected are listed.

13 Configure the network pool for this provider VDC.

You can a create a VXLAN network pool with a default scope, or you can use a custom VXLAN based on a specific NSX Data Center for vSphere or a Geneve pool based on a NSX transport zone. If you are using vSphere networking resources, you can create a provider VDC without a VXLAN network pool.

If you want to use vSphere with Tanzu in VMware Cloud Director, you must select the **NSX Manager and Geneve Network pool** option.

Option	Description
Create a default VXLAN Network Pool	The system creates a VXLAN pool for this provider VDC.
Select VXLAN Network Pool from list	You select a network pool from a list so that you use a custom VXLAN pool based on a specific NSX transport zone.
Select an NSX Manager and Geneve Network pool	You select a network pool from a list so that you use a custom VXLAN pool backed by an NSX transport zone.
No network pool	If you are using vSphere networking resources, you can create a provider VDC without a network pool.

14 Review your choices and click **Finish** to create the provider VDC.

Results

While creating a provider VDC, if you select a resource pool where the ESXi host has an NVIDIA GRID GPU graphics device, the new provider VDC appears with an NVIDIA icon provider VDCs with an NVIDIA icon support virtual GPUs.

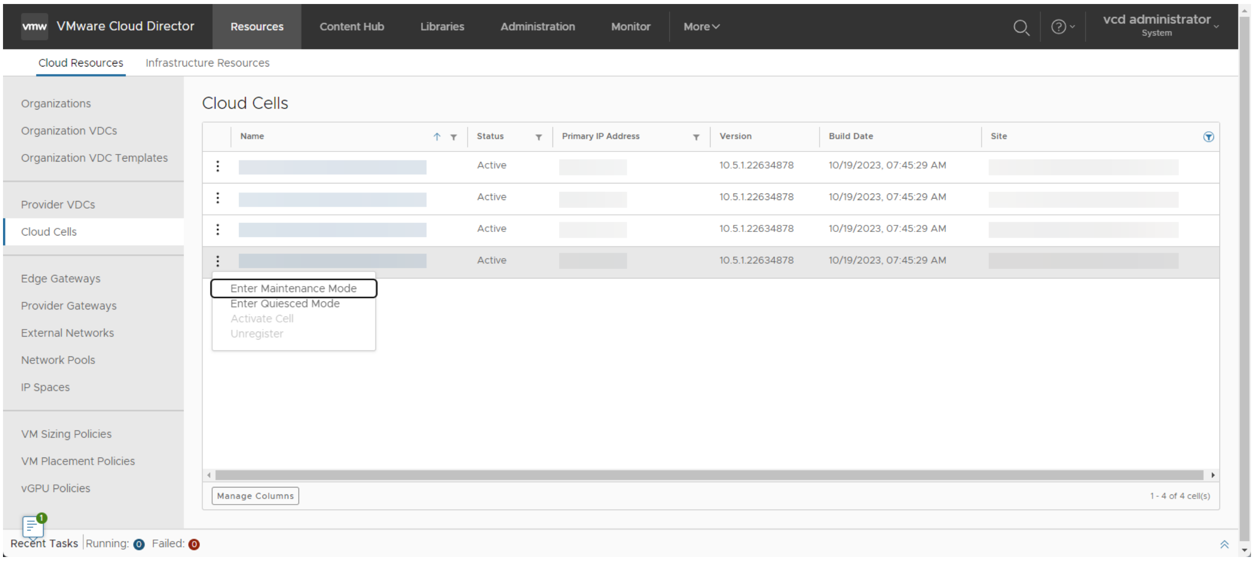
What to do next

You can add secondary resource pools that enable the provider VDC to provide specialized capabilities such as Edge clusters, affinity groups, and hosts with special configurations that some organizations might require. See Add a Resource Pool to a VMware Cloud Director Provider Virtual Data Center.

View and Manage Your VMware Cloud Director Cell Infrastructure

Starting with version 10.5.1, you can use the Service Provider Admin Portal to see the status of your VMware Cloud Director cells and manage your cell infrastructure.

The **Cloud Cells** page displays information about all cells, including cells from other sites. However, you cannot manage the cells from the other sites.



Cloud Cells

Name	Status	Primary IP Address	Version	Build Date	Site
[redacted]	Active	[redacted]	10.5.1.22634878	10/19/2023, 07:45:29 AM	[redacted]
[redacted]	Active	[redacted]	10.5.1.22634878	10/19/2023, 07:45:29 AM	[redacted]
[redacted]	Active	[redacted]	10.5.1.22634878	10/19/2023, 07:45:29 AM	[redacted]
[redacted]	Active	[redacted]	10.5.1.22634878	10/19/2023, 07:45:29 AM	[redacted]

Procedure

1. Log in as a **system administrator** to the Service Provider Admin Portal.
2. From the top navigation bar, under **Resources**, select **Cloud Resources**.
3. In the left panel, click **Cloud Cells**.

   To see more information about the cell, you can click its name. If the cell name is not a link, the cell is from another site.

Change the Status of a Cell

Procedure

1 To change the cell status, click the vertical ellipsis next to the cell name, and select an action.

Option	Description
Enter Maintenance Mode	In maintenance mode, all normal operations stop and the system is unavailable to anyone trying to access VMware Cloud Director. All API calls respond with a `503 Service Unavailable` server error response code. The VMware Cloud Director UI displays a `Maintenance mode is on` message. A load-balancer can use this behavior to configure its monitoring and detect when a cell is unavailable, and as a result, take it out of the pool of available servers. **Important** If you put all of the cells in maintenance mode, you must use an SSH client to log in to the cells to reactivate them because the VMware Cloud Director UI does not work in maintenance mode. See Managing a VMware Cloud Director Cell.
Enter Quiesced Mode	Quiesced cells do not run tasks or other long running activities; but otherwise continue to serve all API calls, console proxy, and MQTT requests. Tasks generated as a result of these API calls run on one of the other active cells. Before transitioning the cell to quiesced mode, VMware Cloud Director finishes all running tasks on this cell. In a single cell environment or a multi-cell environment with no active cells, the tasks continue to queue up until an active cell becomes available. If your VMware Cloud Director environment has a load balancer, the load balancer continues to send requests to that cell.
Activate Cell	Active cells are available to serve API calls and can run tasks.
Unregister	If you want to use a VMware Cloud Director cell in another role, or if you want to remove it from the high availability cluster, you must unregister it.

2 Confirm the action.

Change the Certificates of a Cell

Prerequisites

- Put the cells you want to edit in maintenance mode. See Change the Status of a Cell.
- If you want to change the cell certificate, verify that the certificate you want to use is uploaded to the VMware Cloud Director certificate library. See Import Certificates to the Certificates Library Using Your VMware Cloud Director Service Provider Admin Portal.
  - Verify that the certificate chain in the chosen certificate library item includes your own certificate and all the intermediate certificates.

    Note In rare cases, your certificate chain might also need to include a root certificate authority (CA) certificate. This is not common, and generally, it is not applicable if your CA is one of the well-known certificate authorities whose certificate is distributed using the most modern browsers. Consult with your CA for more information and to determine whether you must append your root certificate.

- **Important** VMware Cloud Director no longer accepts certificates whose signature algorithms use SHA-1.

  Verify that none of the certificates in the certificate chain use SHA-1 as their signature algorithm, for example, `sha1WithRSAEncryption`.

Procedure

1. On the **Cloud Cells** page, click the name of the cell of which you want to change the certificate.
2. Click **Endpoints Configuration**, and click **Edit**.
3. In the **Edit Endpoint Configuration** dialog box, click the edit icon next to the web server SSL certificate or Java Management Extensions (JMX) SSL certificate.

   VMware Cloud Director shows only certificate library items that meet the following criteria.

   - The item is in the certificate library of the `System` organization.
   - The item contains a public key.
   - The item contains a corresponding private key, and if the private key is encrypted, the item must contain a passphrase.
4. Select a certificate from the VMware Cloud Director certificate library.
5. Click **Use Certificate**, and click **Edit**.

   If you are connected directly to a cell, instead of a load balancer, you might need to refresh your web browser to see the newly selected certificate being served.

Results

VMware Cloud Director stops all existing cell connections and changes the certificate. The VMware Cloud Director connection server restarts with the new certificate.

What to do next

To see which cell uses a particular library item, navigate to the certificate library, expand an item to view its details, and scroll down to the **Consumers** section.

Managing Networking Resources in the VMware Cloud Director Service Provider Admin Portal

5

To leverage the networking capabilities of VMware Cloud Director, you can add and manage your infrastructure and cloud networking resources through the Service Provider Admin Portal.

Read the following topics next:

Managing Network Infrastructure Resources in the VMware Cloud Director Service Provider Admin Portal

In the Service Provider Admin Portal, you can add and manage networking infrastructure resources, such as NSX Manager instances, segment profile templates, and NSX Advanced Load Balancer services.

Register an NSX Manager Instance with VMware Cloud Director

To use the networking resources of an NSX Manager instance, you register it with VMware Cloud Director.

Prerequisites

Familiarize yourself with the *NSX Administration Guide*.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **NSX-T Managers** and click **Add**.

3 If you have a multisite VMware Cloud Director deployment, from the **Site** drop-down menu, select the site to which you want to add this NSX Manager instance.

4 Enter a name and, optionally, a description for the NSX Manager instance in VMware Cloud Director.

5 Enter the URL of the NSX Manager instance.

   For example, **`https://`*`FQDN_or_IP_address`***.

6 Enter the network provider scope.

   For global NSX Manager instances which are used in NSX federation, the scope is automatically set to `Global`.

   The network provider scope corresponds to the network fault domain in the network topologies that are used in VDC group networking. It represents the underlying vCenter Server instance with the associated NSX Manager instance. For information on data center group networking, see the *VMware Cloud Director Tenant Guide*.

7 If you want to use the NSX Manager instance as a global manager for NSX federation, toggle on the **Global Manager** option.

8 Enter the user name and password of the NSX Manager **administrator** account.

9 Click **Save**.

What to do next

For information about a creating provider virtual data center backed by NSX, see VMware Cloud Director API Programming Guide for Service Providers.

Modify the NSX Manager Settings in VMware Cloud Director

If the connection information for a registered NSX Manager instance changes, or if you want to change its name and description in VMware Cloud Director, you can modify its settings.

You can modify the settings that you configured when adding the vCenter Server instance. See Register an NSX Manager Instance with VMware Cloud Director.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **NSX-T Managers** and click the name of the NSX Manager instance that you want to modify.

3 In the upper right corner of the **General** tab, click **Edit**.

4 Edit the NSX Manager settings, and click **Save**.

Delete an NSX Manager Instance From VMware Cloud Director

To stop using the resources of a NSX Manager instance, you can remove this vCenter Server instance from your VMware Cloud Director installation.

Prerequisites

Delete all provider virtual data centers that use resources from this NSX Manager instance. See Delete a Provider Virtual Data Center in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **NSX-T Managers**.

3 Click the radio button next to the name of the NSX Manager instance that you want to remove, and click **Delete**.

4 To confirm, click **Delete**.

Adding vCenter Server and NSX Data Center for vSphere Resources to VMware Cloud Director

You can use vSphere in combination with NSX Data Center for vSphere to provide CPU, memory, and storage to run virtual machines on VMware Cloud Director.

VMware Cloud Director can act as an HTTP server between tenants and the underlying vSphere environment.

For information about VMware Cloud Director system requirements and supported versions of vCenter Server and ESXi, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director

You can attach a vCenter Server instance so that its resources become available for use in VMware Cloud Director. You can attach a vCenter Server instance together with its associated NSX-V Manager instance.

For dedicated vCenter Server instances or for those associated with an NSX Manager instance, you can attach a vCenter Server instance alone.

VMware Cloud Director can use a vCenter Server instance either with its associated NSX-V Manager instance or with an NSX Manager instance.

If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must attach the vCenter Server and NSX-V Manager instances together.

If you want VMware Cloud Director to use this vCenter Server instance with an NSX Manager instance, you must attach the vCenter Server instance alone. After you attach the vCenter Server instance alone, you must Register an NSX Manager Instance with VMware Cloud Director.

Note After you attach a vCenter Server instance alone, you cannot add its associated NSX-V Manager instance at a later stage. You can unregister and attach again the vCenter Server instance together with its associated NSX-V Manager instance.

You can attach a vCenter Server instance to any site from your VMware Cloud Director environment.

You can attach a directly accessible vCenter Server instance or attach a vCenter Server instance that is behind a proxy. By using VMware Cloud Director OpenAPI, you can use proxy configurations within VMware Cloud Director to create a proxied connection between a VMware Cloud Director instance and the vCenter Server instance added to it. This way, the VMware Cloud Director and vCenter Server instances can exist in different locations or sites.

To attach a vCenter Server instance that is behind a proxy, first, you must declare a proxy configuration. Then, you must attach a vCenter Server instance, and configure VMware Cloud Director to use the proxy configuration when accessing the vCenter Server instance. You can also attach an NSX solution through a proxy. VMware Cloud Director does not support proxy configurations for NSX Data Center for vSphere. You do not need additional SSL configurations or an additional proxy configuration for the Platform Services Controller the vCenter Server instance is registered with.

Note In a configuration with a proxy, the VMware Cloud Director to proxy communication can use only HTTP. VMware Cloud Director does not support HTTPS proxy configurations. The communication with the vCenter Server instance, tunneled through the proxy, is HTTPS and uses the vCenter Server certificates.

Prerequisites

- If you configured VMware Cloud Director to verify vCenter Server and vSphere SSO certificates, test the connection to the vCenter Server instance and establish a trust relationship. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal..
- If you configured VMware Cloud Director to verify NSX-V Manager or NSX Manager certificates, test the connection to the NSX-V Manager or NSX Manager instance and establish a trust relationship. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal.

Procedure

1 Add the vCenter Server Instance to VMware Cloud Director

   To add a vCenter Server instance toVMware Cloud Director, you must enter the vCenter Server access details.

2 (Optional) Add the Associated NSX Manager Instance to VMware Cloud Director

   If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must add NSX-V Manager access details.

Add the vCenter Server Instance to VMware Cloud Director

To add a vCenter Server instance toVMware Cloud Director, you must enter the vCenter Server access details.

Prerequisites

Familiarize yourself with the vSphere certificate management options. See the vSphere Certificate Management Overview and Certificate Replacement Overview documentation. The VMware Cloud Director certificate strategy depends on your vSphere certificate choices.

vSphere Option	VMware Cloud Director Action
`Using VMCA-signed certificates`	In VMware Cloud Director, trust the CA certificate.
`Using the VMCA certificate as an intermediate certificate`	In VMware Cloud Director, trust the intermediate VMware Certificate Authority (VMCA) certificate.
`Using custom certificates where VMCA is not an intermediate certificate`	Trust the appropriate certificate so that VMware Cloud Director trusts all vSphere components like vCenter Server and ESXi. **Note** You must ensure that VMware Cloud Director trusts all necessary trust anchors.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 In the left pane, click **vCenter Server Instances** and click **Add**.

3 If you have a multisite VMware Cloud Director deployment, from the **Site** drop-don menu, select the site to which you want to add this vCenter Server instance, and click **Next**.

4 Enter a name and, optionally, a description for the vCenter Server instance in VMware Cloud Director.

5 Enter the URL of the vCenter Server instance.

   If the default port is used, you can skip the port number. If a custom port is used, include the port number.

   For example, **`https://`*`FQDN_or_IP_address`*`:`*`<custom_port_number>`***.

6 Enter the user name and password of the vCenter Server **administrator** account.

7 (Optional) To deactivate the vCenter Server instance after the registration, turn off the **Enabled** toggle.

8 Click **Next**.

9 If you haven't already established a trust relationship to the endpoint, on the **Trust Certificate** window confirm if you trust the endpoint.

Option	Description
Trust the connectivity to an endpoint when VMCA is in use	Use this option when in vSphere you are using VMCA-signed certificates or the VMCA as an intermediate certificate. a Review the initial certificate. b If VMCA is not included in the list of certificates, retrieve the additional CA certificates and, depending on your vCenter Server version, select one of the options. ■ For vCenter Server 7.0 and later, to fetch the additional CA certificates, click **Retrieve**. Select the VMCA certificate authority from the updated certificate chain, and trust it. ■ For vCenter Server 6.7 and earlier, you must manually retrieve the CA certificate from vSphere, and use the `Import` option to upload the certificate into the VMware Cloud Director certificates.
Trust the connectivity to an endpoint when VMCA is not in use	Use this option when in vSphere you are using custom certificates where VMCA is not an intermediate certificate a Review the initial certificate. b Determine the trust anchor to trust so that the entire vSphere infrastructure is trusted. Depending on your deployment, you might have to trust additional CAs. You must ensure that VMware Cloud Director trusts all necessary trust anchors. If necessary, use the `Trust Remote Connection` option.
Do not trust the connectivity to this endpoint	a Click **Cancel**. b Repeat Step 5 to Step 8 with a trusted endpoint.

10 (Optional) Skip adding the NSX-V Manager instance that is associated with the vCenter Server instance by turning off the **Configure Settings** toggle and click **Next**.

If you want VMware Cloud Director to use this vCenter Server instance with an NSX-V Manager instance, you must add the vCenter Server instance alone.

Note You cannot add the associated NSX-V Manager instance at a later stage. You can unregister and attach again the vCenter Server instance together with its associated NSX-V Manager instance.

11 If you want to add a tenant dedicated vCenter Server that will not be used as a provider VDC, turn on the **Enable tenant access** toggle.

After you add the vCenter Server instance to VMware Cloud Director, the tenant-related information appears in the details view of the instance.

12 If you want VMware Cloud Director to generate default proxies for the vCenter Server instance and SSO services, turn on the **Generate proxies** toggle.

After you add the vCenter Server instance to VMware Cloud Director, the proxies appear in the **Proxies** tab under **vSphere Resources**.

13 On the **Ready to Complete** page, review the registration details and click **Finish**.

14 If you haven't already trusted the necessary certificates, on the **Trust vSphere Certificate Authority** window, confirm that you trust the certificate so that VMware Cloud Director trusts all vSphere components and the integration with vSphere is complete.

Important If you do not trust the vSphere CA, some VMware Cloud Director features do not work.

You can trust the vSphere CA also after editing the vCenter Server instance.

What to do next

To enable operations acrossvCenter Server instances where the source and destination vCenter Server instances are not the same, verify that the vCenter Server instances trust each other independently of VMware Cloud Director. To view the certificates that a vCenter Server instance trusts, see the Explore Certificate Stores Using the vSphere Client in the *VMware vSphere Product Documentation*. Verify that each vCenter Server instance trusts the other vCenter Server instances that it needs to interact with. See also KB 89906.

(Optional) Add the Associated NSX Manager Instance to VMware Cloud Director

If you want VMware Cloud Director to use this vCenter Server instance with its associated NSX-V Manager instance, you must add NSX-V Manager access details.

Procedure

1 On the **NSX-V Manager** page, leave the **Configure Settings** toggle turned on.

2 Enter the URL of the NSX-V Manager instance.

If the default port is used, you can skip the port number. If a custom port is used, include the port number

For example, **`https://`*`FQDN_or_IP_address`*`:`*`<custom_port_number>`***.

3 Enter the user name and password of the NSX **administrator** account.

4 (Optional) To enable cross-virtual data center networking for the virtual data centers backed by this vCenter Server instance, turn on the **Cross-VDC networking** toggle, and enter the control VM deployment properties and a name for the network provider scope.

The control VM deployment properties are used for deploying an appliance on the NSX-V Manager instance for cross-virtual data center networking components like a universal router.

Option	Description
Network Provider Scope	Corresponds to the network fault domain in the network topologies of the data center groups. For example, `boston-fault1`. For information about managing cross-virtual data center groups, see the *VMware Cloud Director Tenant Guide*.
Resource Pool Path	The hierarchical path to a specific resource pool in the vCenter Server instance, starting from the cluster, *Cluster/Resource_Pool_Parent/Target_Resource* . For example, `TestbedCluster1/mgmt-rp`. As an alternative, you can enter the Managed Object Reference ID of the resource pool. For example, `resgroup-1476`.
Datastore Name	The name of the datastore to host the appliance files. For example, `shared-disk-1`.
Management Interface	The name of the network in vCenter Server or port group used for the HA DLR management interface. For example, `TestbedPG1`.

5 Click **Next**.

6 If the endpoint does not have a trusted certificate, on the **Trust Certificate** window confirm if you trust the endpoint.

- To add the endpoint to the centralized certificate storage area and continue, click **Trust** .
- If you do not trust this endpoint, click **Cancel** and repeat Step 2 to Step 4 with a trusted endpoint.

7 Activate or deactivate the access configuration settings.

8 On the **Ready to Complete** page, review the registration details and click **Finish**.

What to do next

- Assign the NSX License Key in vCenter Server.
- Create a Provider Virtual Data Center in Your VMware Cloud Director.

Discovering and Adopting VMs in VMware Cloud Director

In the default configuration, a VMware Cloud Director organization VDC discovers virtual machines (VMs) that are created in any vCenter Server resource pool that backs the VDC.

After the **system administrator** grants you access to a discovered VM, you can reference the VM when you compose or recompose a vApp.

Each discovered VM is given a name that is derived from the name of the vCenter Server VM and a prefix specified by your organization administrator.

If you want to discover additional VMs, a **system administrator** can use the VMware Cloud Director API to create organization VDCs that adopt specified resource pools available from a provider VDC. vCenter Server VMs in these adopted resource pools appear in the new VDC as discovered VMs, and are candidates for adoption.

Note Virtual machines with IDE hard drives are discovered only if they are in powered off state.

If one or more vCenter VMs are not discovered by VMware Cloud Director, you can investigate the possible reasons by debugging the vCenter VM Discovery. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Activating VM Discovery

VM discovery is active by default. You can control VM discovery at three levels.

- Global setting at the cell level that **system administrators** can modify by using the Service Provider Admin Portal.

  a From the top navigation bar, select **Administration**.

  b In the left panel, under **Settings**, select **General**.

  c Edit the **Other** section.

  d Toggle the **VM discovery enabled** option.

  If the global-level setting is deactivated, then VM discovery is deactivated, regardless of the organization-level or VDC-level setting. If you want to override the global-level settings, see Activating VM Discovery by Using the VMware Cloud Director API section.

- Organization-level setting that **system administrators** can modify.

  a From the top navigation bar, select **Resources**.

  b In the left panel click **Organizations** and select the organization for which you want to modify the setting.

  c Under **Configure**, select **General**, and click to edit the **Other** section.

  d Select the VM discovery option for all VDCs in the organization.

  If the organization-level setting is deactivated, then VM discovery is deactivated on all VDCs in the organization, regardless of the VDC-level setting. If you want to override the organization-level settings, see Activating VM Discovery by Using the VMware Cloud Director API section.

- VDC-level setting that **system administrators** can modify.

  a From the top navigation bar, select **Resources**.

  b In the left panel click **Organization VDCs** and select the VDC for which you want to modify the setting.

  c Select the **General** tab and click **Edit** to modify the **Other** section.

  d Select the VM discovery option for the VDC.

Activating VM Discovery by Using the VMware Cloud Director API

VM discovery is active by default. To deactivate VM discovery for all organizations, a system administrator must update the value of the `VmDiscoveryEnabled` setting in the system's `GeneralSettings`. To deactivate VM discovery for all VDCs in an organization, an organization administrator must update the value of the `VmDiscoveryEnabled` setting in the `GeneralOrgSettings` for that organization. To deactivate VM discovery for an individual organization VDC, an organization administrator must update the value of the `VmDiscoveryEnabled` setting in the `AdminVdc` that represents the organization VDC.

To override the VM discovery default behavior, use the VMware Cloud Director API `/api/admin/extension/settings/general` to set the `AllowOverrideOfVmDiscoveryByOrgAndOVDC` parameter to `true`. When you set the parameter to `true`, you can modify the VM discovery settings at the organization and organization VDC level even if VM discovery is deactivated at the global level.

```
allow-override-of-vm-discovery-by-org-and-orgvdc = true
```

The `AllowOverrideOfVmDiscoveryByOrgAndOVDC` parameter is set to `null` by default and the global settings override all lower-level settings.

Using a VM from a Discovered VM

After the system administrator grants you access, you can use a discovered VM in the same ways you can use any other VM. For example, you can specify it when you build a new vApp. You can also clone a discovered VM or modify its name, description, or lease settings without triggering the adoption process.

Adopting a Discovered VM

You can adopt a discovered VM by changing its VM network. After you adopt a discovered VM, the system imports it and treats it as though it was created in VMware Cloud Director. When you retrieve an adopted VM with a VMware Cloud Director API request, the VM includes an element named `autoNature`. If the discovered VM was adopted or created in VMware Cloud Director, this element has a value of `false` . You cannot revert an adopted VM to a discovered VM.

Note Adopting a VM does not retain the VM reservation, limit, and shares settings that are configured in vCenter Server. Imported VMs obtain their resource allocation settings from the organization virtual data center (VDC) on which they reside.

Assign the NSX License Key in vCenter Server

If you attached a vCenter Server instance to its associated NSX-V Manager instance, you must assign a license key for the NSX-V Manager instance that supports VMware Cloud Director networking.

Prerequisites

Verify that you are logged in as a **system administrator**.

Procedure

1. From a vSphere Client that is connected to the vCenter Server system, select **Home > Licensing**.
2. For the report view, select **Asset**.
3. Right-click the NSX Manager asset and select **Change license key**.
4. Select **Assign a new license key** and click **Enter Key**.
5. Enter the license key, enter an optional label for the key, and click **OK**.

   Use the NSX Manager license key you received when you purchased VMware Cloud Director. You can use this license key in multiple vCenter Server instances.
6. Click **OK**.

Modify NSX Manager Settings in Your VMware Cloud Director

If the connection information for a registered NSX-V Manager instance changes, or if you want to change its name and description in VMware Cloud Director, you can modify its settings.

You can modify the settings that you configured when adding the NSX-V Manager instance. See (Optional) Add the Associated NSX Manager Instance to VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left pane, click **vCenters** and click the name of the vCenter Server instance that is associated with the target NSX-V Manager instance.
3. In the upper-right corner of the **NSX-V Manager Info** section, click **Edit**.
4. Modify the NSX-V Manager hostname and administrator credentials, and click **Save**.
5. (Optional) To enable cross-virtual data center networking for the virtual data centers backed by this vCenter Server instance, turn on the toggle, and then enter the control VM properties and a name for the network provider scope.

   The control VM properties are used for deploying an appliance on the NSX-V Manager instance for cross-virtual data center networking components, such as a universal router.

Parameter	Description
Resource Pool Path	The hierarchical path to a specific resource pool in the vCenter Server instance, starting from the cluster, *Cluster/Resource_Pool_Parent/ Target_Resource* . For example, `TestbedCluster1/mgmt-rp`. As an alternative, you can enter the Managed Object Reference ID of the resource pool. For example, `resgroup-1476`.
Datastore Name	The name of the datastore to host the appliance files. For example, `shared-disk-1`.

Parameter	Description
Management Interface	The name of the network in vCenter Server or port group used for the HA DLR management interface. For example, **`TestbedPG1`**.
Network Provider Scope	Corresponds to the network fault domain in the network topologies of the data center groups. For example, **`boston-fault1`**. For information about managing cross-virtual data center groups, see the *VMware Cloud Director Tenant Guide*.

NSX API Rate Limits in VMware Cloud Director

When you use the NSX API to manage the networking resources of VMware Cloud Director, there are some limitations to consider.

The NSX API service has three settings that control the rate of incoming API requests.

While it is possible to configure these rate limits using the `/api/v1/node/services/http` API, it is not recommended. Instead, design your API client to gracefully deal with situations where limits are exceeded.

Per-client rate limit

If a client makes more requests than this limit in one second, the API server refuses to service the request and returns an `HTTP 429 Too Many Requests` Error. By default, this limit is 100 requests per second.

Per-client concurrency limit

This is the maximum number of outstanding requests that a client can have. For example, a client can open multiple connections to NSX and submit operations on each connection. When this limit is exceeded, the server returns a `429 Too Many Requests` error to the client. By default, this limit is 40 concurrent requests.

An overall maximum number of concurrent requests.

This is the maximum number of API requests that can be in process on the server. If the server is at this limit, additional requests are refused and the HTTP error `503 Service Unavailable` returns to the client. By default, this limit is 199 concurrent requests.

For details, see the documentation for NSX REST API at VMware {code}.

Using NSX Manager Segment Profile Templates in VMware Cloud Director

Starting with VMware Cloud Director 10.3.2, you can define segment profile templates to be applied to organization VDC networks and to vApp networks upon their creation or as an update.

Segment Profile Templates

A segment profile template is a set of NSX segment profiles that are created in NSX Manager and used by VMware Cloud Director. In VMware Cloud Director, you can apply segment profile templates to organization VDC networks and vApp networks upon their creation or as an update.

Depending on your environment needs, you can set segment profile templates that are applied at different levels.

You can define global segment profile templates to be applied to all new organization VDC networks or vApp networks within a specific site.

You can set organization VDC network and vApp network segment profile templates at the organization VDC level. These VDC segment profile templates would override any global default segment profile templates.

You can also configure and apply a specific segment profile template when you create a new organization VDC network or when you update it.

When you create or update a segment profile template, the segment profiles from the source NSX Manager instance are synced to all other on-premises NSX Manager instances that are registered with VMware Cloud Director and are applied globally.

Segment Profiles

Segment profiles include layer 2 configuration details for segments and segment ports. There are several types of segment profiles: IP discovery, MAC discovery, SpoofGuard, quality of service (QoS), and segment security. When you create a segment profile template, you can include only one segment profile of each type. For more details on each type of segment profile, see Segment Profiles in *NSX Administration Guide*.

Create a Segment Profile Template in VMware Cloud Director

You can combine NSX Manager segment profiles to define segment profile templates in VMware Cloud Director.

Prerequisites

Verify that you have created segment profiles in NSX Manager.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 Under **NSX-T**, click **Segment Profile Templates**.

3 Select the **Templates** tab and click **New**.

4 If you are managing a multisite environment, from the drop-down menu, select a site in which to create the new segment profile template.

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

6 From the list, select the NSX Manager instance with the segment profiles that you want to use as a source for this template.

7 Select a segment profile from each type to add to the template.

   If you don't select a segment profile for a given type, the NSX Manager default is included in the template.

8 Review the **Ready to Complete** page, and click **Finish**.

What to do next

You can edit the segment profile template as needed.

Set a Global Default Segment Profiles Template in VMware Cloud Director

You can set global default segment profiles to be applied to all VDC networks and all vApp networks in a VMware Cloud Director environment upon their creation.

The global default segment profile templates apply to a network if you don't configure custom segment profiles at the time of the network creation and if you haven't set a default segment profile template for the organization VDC in which you are creating the network.

Prerequisites

Verify that you created custom segment profiles in NSX Manager.

Procedure

1 From the top navigation bar, under **Resources**, click **Infrastructure Resources**.

2 Under **NSX-T**, click **Segment Profile Templates**.

3 Click the **Global Defaults** tab.

4 If you are managing a multisite environment, select the site for which you want to set a global template.

5 Click **Edit**.

6 To set a default template for VDC networks, select a template from the drop-down menu.

7 To set a default template for vApp networks, select a template from the drop-down menu.

8 Click **Save**.

Results

VMware Cloud Director copies the segment profiles that you select from the source NSX Manager instance to all other NSX Manager instances that are registered in this environment and applies them globally.

What to do next

You can edit the global default segment profile template as needed.

Managing NSX Advanced Load Balancing in VMware Cloud Director

Starting with version 10.2, VMware Cloud Director provides load balancing services by leveraging the capabilities of VMware NSX Advanced Load Balancer.

As a **system administrator**, you can enable and configure access to load balancing services for virtual data centers backed by NSX.

Load balancing services are associated with NSX edge gateways, which can be scoped either to an organization VDC backed by NSX or to a data center group with NSX network provider type.

After you deploy and configure NSX Advanced Load Balancer to use with your NSX deployment, you register Controllers with VMware Cloud Director.

For information on how to configure NSX Advanced Load Balancer with NSX, see Avi Integration with NSX.

To use the virtual infrastructure provided by NSX Advanced Load Balancer, register your NSX Cloud instances with VMware Cloud Director. Controllers serve as a central control plane for load balancing services. After you register your controllers, you can manage them directly from VMware Cloud Director.

The load balancing compute infrastructure provided by NSX Advanced Load Balancer is organized into service engine groups. You can assign more than one service engine group to an NSX edge gateway in VMware Cloud Director. All service engine groups that are assigned to a single edge gateway use the same network.

A service engine group has a unique set of compute characteristics that you define upon creation.

After a **system administrator** assigns a service engine group to an edge gateway, an **organization administrator** can create and configure virtual services that run in a specific service engine group.

Register a Controller Instance in VMware Cloud Director

To integrate VMware Cloud Director with your NSX Advanced Load Balancer deployment, you register Controller instances with your VMware Cloud Director instance.

Controller instances serve as a central control plane for the load-balancing services provided by NSX Advanced Load Balancer.

Prerequisites

Install and configure NSX Advanced Load Balancer with your NSX instance.

For information about configuring NSX Advanced Load Balancer with NSX, see Avi Integration with NSX.

Note The FQDN or IP address that you use to register NSX Manager with NSX Advanced Load Balancer must match the FQDN or IP address of the NSX Manager instance that you used to register NSX with VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Click **NSX-ALB** and then click **Controllers**.
3. To add a controller, click **Add**.
4. If you are using a multisite deployment, from the drop-down menu, select a site in which to register the Controller.
5. Register the Controller instance.
   a. Enter a meaningful name and, optionally, a description for the Controller instance.
   b. Enter the URL of the Controller.

      For example, `https://FQDN-or-IP-address`.
   c. Enter the user name and password for the default predefined NSX Advanced Load Balancer **system administrator** user.

      Note The default predefined NSX Advanced Load Balancer **system administrator** role has system level credentials that allow VMware Cloud Director to make infrastructure and application changes in NSX Advanced Load Balancer.
   d. Click **Save**.

Results

The Controller instance appears in the list as enabled.

What to do next

Register an NSX Cloud in VMware Cloud Director.

Register an NSX Cloud in VMware Cloud Director

To use the virtual infrastructure provided by NSX Advanced Load Balancer, register your NSX Cloud instances with VMware Cloud Director.

An NSX Cloud is a service provider-level construct that consists of an NSX Manager and an NSX transport zone.

NSX Manager provides a system view and is the management component of NSX. An NSX transport zone dictates which hosts and virtual machines can participate in the use of a particular network.

If there are multiple transport zones managed by the same NSX Manager, then a separate NSX Cloud encapsulates each pair of NSX Manager and NSX transport zone instances.

An NSX Cloud has a one-to-one relationship with a network pool backed by an NSX transport zone.

Prerequisites

- Install and configure NSX Advanced Load Balancer with your NSX instance. For detailed information on how to configure NSX Advanced Load Balancer with NSX, see Avi Integration with NSX.

  Note Enable DHCP on the NSX tier-1 gateway upon its creation.

- Register a Controller Instance in VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Click **NSX-ALB** and then click **NSX-T Clouds**.
3. To add an NSX cloud, click **Add**.
4. From the drop-down menu, select a Controller instance for which to create the NSX Cloud.
5. Enter a name and, optionally, a description for the NSX Cloud.
6. Select an available Cloud from the list.
7. To import the cloud, click **Add**.

Results

The imported cloud appears in the list of available NSXClouds.

What to do next

Import a Service Engine Group in Your VMware Cloud Director.

Import a Service Engine Group in Your VMware Cloud Director

To provide virtual service management capabilities to your tenants, import service engine groups to your VMware Cloud Director deployment.

A service engine group is an isolation domain that also defines shared service engine properties, such as size, network access, and failover.

Resources in a service engine group can be used for different virtual services, depending on your tenant needs. These resources cannot be shared between different service engine groups.

You can manage and update service engine groups by using NSX Advanced Load Balancer. After you update a service engine group in NSX Advanced Load Balancer, you must sync it to update its settings in the VMware Cloud Director UI.

Only an imported service engine group can be assigned to an edge gateway.

To import a service engine group, associate it with an NSX Cloud that is already registered with your VMware Cloud Director instance.

Note If you are using NSX Advanced Load Balancer with a **Standard** feature set, before importing a service engine group, consider configuring it with elastic HA active/active mode with 1 active service engine and 1 buffer service engine to ensure a seamless transition to **Premium**, if necessary. For details, see *VMware NSX Advanced Load Balancer Installation Guide*.

Prerequisites

- Install and configure NSX Advanced Load Balancer with your NSX instance. For detailed information on how to configure NSX Advanced Load Balancer with NSX, see Avi Integration with NSX.
- Register a Controller Instance in VMware Cloud Director.
- Register an NSX Cloud in VMware Cloud Director.
- Verify that you acquired a NSX Advanced Load Balancer Enterprise Edition license. See *VMware NSX Advanced Load Balancer Administration Guide*.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Click **NSX-ALB** and then click **Service Engine Groups**.
3. To import a service engine group, click **Add**.
4. From the drop-down menu, select an NSX Cloud.
5. Select a reservation model.
   - To assign the service engine group to a single edge gateway, select **Dedicated**.
   - To share the service engine group between several edge gateways, select **Shared**.
6. Enter a name and, optionally, a description, for the service engine group.
7. From the drop-down menu, select a feature set.

Option	Description
Standard	The standard feature set provides the load balancing features included in VMware NSX Advanced Load Balancer Basic Edition.
Premium	The premium feature set provides some of the features included in VMware NSX Advanced Load Balancer Enterprise Edition, such as, for example, additional load balancing pool algorithm types and pool persistence profiles, virtual service analytics, pool analytics, multiple virtual service ports, and additional virtual service application profile types.

8. Select a service engine group instance.
9. Click **Add**.

What to do next

Enable load balancing on the edge gateway and assign the service engine group to the edge gateway. See Managing NSX Advanced Load Balancing on an NSX Edge Gateway in VMware Cloud Director.

Sync a Service Engine Group in Your VMware Cloud Director

To update the settings of an imported service engine group in VMware Cloud Director, you must sync it with NSX Advanced Load Balancer.

You can manage and update service engine groups by using NSX Advanced Load Balancer. After you update a service engine group in NSX Advanced Load Balancer, you must sync it to update its settings in the VMware Cloud Director UI.

Syncing a service engine group updates the local record of the group's high availability mode and the maximum number of virtual services that the service engine group supports.

Important After you sync a service engine group, if the new maximum number of supported virtual services is lower than the number of reserved virtual services, the service engine group is marked as overallocated.

If a service engine group is overallocated, the creation of a new virtual service might fail, even if the edge gateway on which you create the virtual service has enough reserved capacity.

To avoid failure of virtual service creation, when you edit the settings of a service engine group, do not reduce the maximum number of supported virtual services below the number of initially reserved virtual services.

Prerequisites

Import a Service Engine Group in Your VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Select **NSX-ALB** and then click **Service Engine Groups**.
3. Select a service engine group and click **Sync**.

Results

The settings of the service engine group are updated.

Edit the Reservation Model and the Feature Set of a Service Engine Group in Your VMware Cloud Director

If necessary, you can change the reservation model and the feature set of a service engine group in VMware Cloud Director.

Prerequisites

- Import a Service Engine Group in Your VMware Cloud Director.

- If you want to edit the feature set of the service engine group, verify that it is assigned to an edge gateway.
- If you want to downgrade the feature set of the service engine group to **Standard** from **Premium**, verify that there are no virtual services and no load balancer server pools configured on the edge gateway to which it is assigned.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. Select **NSX-ALB** and then click **Service Engine Groups**.
3. Select a service engine group and, under General, click **Edit**.
4. From the drop-down menu, edit the reservation model.
   - To assign the service engine group to a single edge gateway, select **Dedicated**.
   - To share the service engine group between several edge gateways, select **Shared**.
5. Edit the name and the description of the service engine group.
6. From the drop-down menu, edit the feature set of the service engine group.

Option	Description
Standard	The standard feature set provides the load balancing features included in VMware NSX Advanced Load Balancer Basic Edition.
Premium	The premium feature set provides some of the features included in VMware NSX Advanced Load Balancer Enterprise Edition, such as, for example, additional load balancing pool algorithm types and pool persistence profiles, virtual service analytics, pool analytics, multiple virtual service ports, and additional virtual service application profile types.

7. Click **Save**.

Managing Cloud Networking Resources in the VMware Cloud Director Service Provider Admin Portal

In the Service Provider Admin Portal, you can add and manage cloud networking resources, such as network pools, external networks, provider gateways, and IP spaces.

Network Pools in VMware Cloud Director

A network pool is a group of undifferentiated networks that is available for use in a VMware Cloud Director organization VDC to create vApp networks and certain types of organization VDC networks.

A network pool is backed by vSphere network resources, such as VLAN IDs or port groups, by NSX Data Center for vSphere resources, or by NSX resources.

VMware Cloud Director uses network pools to create NAT-routed and internal organization VDC networks and all vApp networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Each organization VDC in VMware Cloud Director can have one network pool. Multiple organization VDCs can share a network pool. The network pool for an organization VDC provides the networks created to satisfy the network quota for an organization VDC.

VXLAN Network Pools in Your VMware Cloud Director

Every VMware Cloud Director provider VDC that is backed by NSX Data Center for vSphere includes a VXLAN network pool.

When you create a provider VDC that is backed by NSX Data Center for vSphere, you can associate that provider VDC with an existing VXLAN network pool, or you can create a VXLAN network pool for the provider VDC.

A newly created VXLAN network pool is given a name derived from the name of the containing provider VDC and attached to it at creation. You cannot delete or modify this network pool. If you rename a provider VDC, its VXLAN network pool is automatically renamed.

Note To ensure optimal network performance across your infrastructure, create one VXLAN network pool and associate it with all your provider VDCs upon their creation.

VMware Cloud Director VXLAN networks are based on the IETF VXLAN standard, and provide various benefits.

- Logical networks spanning layer 3 boundaries
- Logical networks spanning multiple racks on a single layer 2
- Broadcast containment
- Higher performance
- Greater scale (up to 16 million network addresses)

For more information about VXLAN networks in a VMware Cloud Director environment, see the *NSX Administration Guide*.

Create a Network Pool Backed by an NSX Data Center for vSphere Transport Zone in Your VMware Cloud Director

To register an NSX Data Center for vSphere transport zone for VMware Cloud Director to use, add a VXLAN-backed network pool.

Prerequisites

Create an NSX Data Center for vSphere transport zone on any vCenter Server registered to VMware Cloud Director. See the *NSX Administration Guide*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Network Pools** and click **New**.

3 Enter a name and, optionally, a description for the new network pool, and click **Next**.

4 Select **VXLAN-backed** and click **Next**.

5 Select a vCenter Server instance to specify the VXLAN transport zone to be used by this network pool, and click **Next**.

6 Select an NSX Data Center for vSphere transport zone to back the new network pool, and click **Next**.

> **Note** To create a universal network pool for cross-virtual data center networking, select a **UNIVERSAL_VXLAN** type transport zone.

7 Review the network pool settings and click **Finish**.

What to do next

Create an organization VDC network that is backed by the network pool or associate the network pool with an organization VDC and create vApp networks.

Geneve Network Pools in Your VMware Cloud Director

Every VMware Cloud Director provider VDC that is backed by NSX includes a Geneve network pool.

Geneve is the network virtualization standard that provides the overlay capability in NSX.

When you create a provider VDC that is backed by NSX, you can associate that provider VDC with an existing Geneve network pool, or you can create a Geneve network pool for the provider VDC.

VMware Cloud Director Geneve networks provide a number of benefits.

- Logical networks spanning layer 3 boundaries
- Logical networks spanning multiple racks on a single layer 2
- Broadcast containment
- Higher performance
- Greater scale (up to 16 million network addresses)

Create a Network Pool Backed by an NSX Transport Zone in Your VMware Cloud Director

To register an NSX transport zone for VMware Cloud Director to use, create a Geneve-backed network pool.

Prerequisites

Create an NSX transport zone that is overlay backed. For more information on the transport zone creation and the Generic Network Virtualization Encapsulation, called Geneve overlay, see the NSX product documentation.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Network Pools** and click **New**.
3. Enter a name and, optionally, a description for the new network pool, and click **Next**.
4. Select **Geneve-backed** and click **Next**.
5. Select an NSX Manager instance to provide the transport zone for this network pool, and click **Next**.
6. Select an NSX transport zone and click **Next**.
7. Review the network pool settings and click **Finish**.

What to do next

Create an organization VDC network that is backed by the network pool or associate the network pool with an organization VDC and create vApp networks.

Create a Network Pool Backed by VLAN IDs in Your VMware Cloud Director

To register vSphere VLAN IDs for VMware Cloud Director to use, add a VLAN-backed network pool. A VLAN-backed network pool provides the security, scalability, and performance for organization VDC networks.

Prerequisites

Verify that a range of VLAN IDs and a vSphere distributed switch are available in vSphere. The VLAN IDs must be valid IDs that are configured in the physical switch to which the ESXi servers are connected.

Caution The VLANs must be isolated at the layer 2 level. Failure to isolate properly the VLANs can cause a disruption on the network.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Network Pools** and click **New**.
3. Enter a name and, optionally, a description for the new network pool, and click **Next**.
4. Select **VLAN-backed** and click **Next**.
5. Select a vCenter Server instance to specify the distributed virtual switch to be used by this network pool and click **Next**.
6. Enter a VLAN ID range and click **Next**.
7. Select a distributed switch for the network pool and click **Next**.
8. Review the network pool settings and click **Finish**.

What to do next

Create an organization VDC network that is backed by the network pool or associate the network pool with an organization VDC and create vApp networks.

Create a Network Pool Backed by vSphere Port Groups in Your VMware Cloud Director

To register vSphere port groups for VMware Cloud Director to use, add a network pool backed by port groups.

Unlike other types of network pools, a port group-backed network pool does not require a vSphere distributed switch and can support port groups associated with third-party distributed switches.

Caution The port groups must be isolated from all other port groups at layer 2. The port groups must be physically isolated or must be isolated by using VLAN tags. Failure to isolate properly the port groups can cause a network disruption.

Prerequisites

Port groups with or without VLAN trunking are supported

Verify that one or more port groups are available in your vSphere environment. The port groups must be available on each ESXi host in the cluster, and each port group must use only a single VLAN.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Network Pools** and click **New**.

3 Enter a name and, optionally, a description for the new network pool, and click **Next**.

4 Select **Portgroup-backed** and click **Next**.

5 Select a vCenter Server instance to provide port groups to be used by this network pool, and click **Next**.

6 Select one or more port groups and click **Next**.

   You can create one network for each port group.

7 Review the network pool settings and click **Finish**.

What to do next

Create an organization VDC network that is backed by the network pool or associate the network pool with an organization VDC and create vApp networks.

External Networks in Your VMware Cloud Director

A VMware Cloud Director external network provides an uplink interface that connects networks and virtual machines in the system to a network outside of the system, such as a VPN, a corporate intranet, or the public Internet. Only a **system administrator** can create an external network.

If you have more than one vCenter Server instance registered to the system, you can create multiple external networks, each backed either by a vSphere network, an NSX segment that is configured either with a VLAN or an overlay transport zone.

VMware Cloud Director supports IPv4 and IPv6 external networks. Dual-stack external networks are not supported.

Note The range of IP addresses that you define when you create the external network are allocated either to an edge gateway or to the virtual machines that are directly connected to the network. Because of this, the IP addresses must not be used outside of VMware Cloud Director.

External Networks Backed by vSphere Networks

This type of external networks can be backed either by a single vSphere network, or by multiple vSphere networks.

- External networks backed by a single vSphere instance.

  To provide each consumer of the external network with a non-overlapping set of IP addresses on the vSphere network, the **system administrator** must configure the IP ranges on the underlying VLAN manually.

- External networks backed by multiple vSphere networks.

  An external network can be backed by multiple vSphere networks. This approach can simplify the IP address management in VMware Cloud Director. You can modify the properties of an external network to change its network backings.

  External networks backed by multiple vSphere networks have several constraints.

  - A network can have at most one backing vSphere network on each VMware Cloud Director instance registered to the system.
  - All backing network switches must be of the same type, either vSphere Distributed Switch or standard switch.
  - Each network must be on a different switch.

External networks backed by an NSX Segment

An external network can be backed by an imported NSX segment that is configured either with a VLAN or an overlay transport zone. In NSX, segments are virtual layer 2 domains. A segment was earlier called a logical switch.

Provider Gateways

In VMware Cloud Director 10.5, tier-0 gateways are replaced by provider gateways. See Managing Provider Gateways in Your VMware Cloud Director.

Add an External Network That Is Backed by vSphere Resources to Your VMware Cloud Director

By adding an external network, you can register vSphere network resources for VMware Cloud Director to use. You can create organization VDC networks that connect to an external network.

You can add an IPv4 or IPv6 external network.

Prerequisites

Verify that a vSphere port group is available with or without VLAN trunking. Elastic port groups with static port binding ensure optimal performance.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **External Networks** and click **New**.
3. Select **vSphere Resources**, select the type of port groups to back the network, and click **Next**.
4. Enter a name and, optionally, a description for the new external network.
5. Select the port groups to back the external network and click **Next**.
6. Configure at least one subnet and click **Next**.
   a. To add a subnet, click **Add**.
   b. 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`.
   c. (Optional) Enter the DNS settings.
   d. Configure a static IP pool by adding at least one IP range or IP address.
   e. Click **OK**.
   f. (Optional) To add another subnet, repeat this step.
7. Review the network settings and click **Finish**.

What to do next

You can create an organization VDC network that connects to the external network.

Add an External Network Backed by an NSX Segment to Your VMware Cloud Director

In VMware Cloud Director, you can create an external network that is backed by an NSX segment.

In NSX, segments are virtual layer 2 domains. A segment was earlier called a logical switch.

Adding an NSX segment enables the creation of direct organization VDC networks backed by NSX.

An NSX segment can be backed either by a VLAN transport zone or by an overlay transport zone.

Prerequisites

- Verify that you are a **system administrator**.
- Verify that you created the segment in NSX Manager. For more information segments, see *NSX Administration Guide*.

Procedure

1. Log in to the VMware Cloud Director Service Provider Admin Portal.
2. From the top navigation bar, select **Resources** and click **Cloud Resources**.
3. In the left pane, click **External Networks** and click **New**.
4. On the **Backing Type** page, select **NSX-T Segments** and a registered NSX Manager instance to back the network, and click **Next**.
5. Enter a name and, optionally, a description for the new external network.
6. Select an NSX segment from the list to import and click **Next**.
7. Configure at least one subnet and click **Next**.
   a. To add a subnet, click **New**.
   b. Enter a gateway CIDR.
   c. To enable, select the **State** checkbox.
   d. Configure a static IP pool by adding at least one IP range or IP address.
   e. Click **Save**.
   f. (Optional) To add another subnet, repeat steps #unique_83/unique_83_Connect_42_substep_4AA8D1D130414D93B35EA2DFF3A2F64D to #unique_83/unique_83_Connect_42_substep_A984C92A52CB42FD84DCB8E3F44DBDF7.
8. Review the network settings and click **Finish**.

Managing Provider Gateways in Your VMware Cloud Director

As a VMware Cloud Director **service provider**, you can use provider gateways to expose the IP spaces that you allocate to tenants by creating IP space uplinks.

Starting with version 10.4.1, importing an NSX Tier-0 Gateway to VMware Cloud Director is replaced by adding a provider gateway.

Unlike tier-0 gateways that you can dedicate to specific edge gateways, you can dedicate a provider gateway to an organization by making the provider gateway private. This makes possible connecting more than one edge gateway to a single private provider gateway.

As a **service provider**, you can use provider gateways to expose the IP spaces that you allocate to tenants by creating IP space uplinks. Associating IP spaces with a provider gateway increases tenant visibility and provides control over default service configuration, control over routing rules, and dynamic routing configuration.

Organization administrators can view general information about the IP spaces to which their organization has access through IP uplinks, and a diagram for the network topology that includes both the provider gateways and the edge gateways in their environment.

Add a Provider Gateway to Your VMware Cloud Director

To register NSX network resources for VMware Cloud Director to use, you can add a provider gateway to VMware Cloud Director.

Prerequisites

To add a provider gateway, first you must create a tier-0 gateway in NSX Manager to back it. You can create the tier-0 gateway in the NSX Manager UI or by using the NSX Policy API.

If you want to add a tier-0 gateway that is backed by a VRF gateway in NSX, you must also create a VRF gateway that is linked to the tier-0 gateway.

- Create a tier-0 gateway in the NSX Manager UI.

  a Log in with administrative privileges to the NSX Manager instance.

  b Click **Networking**, click **Tier-0 Gateways**, and click **Add Gateway > Tier-0**.

  c Enter a name for the tier-0 gateway.

  d Select a High Availability mode.

  > **Note** By default, the active-active mode is used. In the active-active mode, the traffic is load balanced across all members. In active-standby mode, an elected active member processes the traffic. If the active member fails, a new member becomes active.

  e Select an existing NSX edge cluster from the drop-down menu to back this tier-0 gateway, and click **Save**.

- If you want to add a tier-0 gateway that is backed by a VRF gateway in NSX, create a VRF gateway that is linked to the tier-0 gateway.

  a Log in with administrative privileges to the NSX Manager instance.

  b Click **Networking**, click **Tier-0 Gateways**, and click **Add Gateway > VRF**.

  c Enter a name for the VRF gateway.

  d Select the tier-0 gateway to which to connect the VRF gateway.

  e Click **Save**.

Procedure

1 Log in to the VMware Cloud Director Service Provider Admin Portal.

2 From the top navigation bar, select **Resources** and click **Cloud Resources**.

3 In the left pane, click **Provider Gateways** and click **New**.

4 If you are running a multisite environment, select a site in which to register the new provider gateway, and click **Next**.

5 Select a registered NSX Manager instance to back the gateway, and click **Next**.

6 Enter a name and, optionally, a description for the new provider gateway.

7 Select an IP management method for the new provider gateway and click **Next**

   - To use IP Space Management for the provider gateway, select **Use IP Spaces**.
   - To use the legacy IP management UI for the provider gateway, select **Use IP Blocks (legacy)**.

8 If you selected **IP Spaces** as an IP management method, select the ownership for the provider gateway.

   - To make the provider gateway accessible to all organizations within your environment, select **Public**.
   - To dedicate the private gateway to a single organization, select **Private**, and, from the drop-down menu, select an organization to which to dedicate the gateway.

9 Select a tier-0 router or a VRF gateway to connect to the provider gateway, and click **Next**.

10 If you selected **IP Blocks** as an IP management method, configure one or more IP blocks to allocate to the gateway, and click **Next**.

   a To add an IP block, click **New**.

   b Enter an IP block for the gateway.

   c To enable, select the **State** check box.

   d Configure a static IP pool by adding at least one IP range or IP address.

e Click **Save**.

f (Optional) To add another IP block, repeat steps 10.a to 10.e.

11 Review the network settings and click **Finish**.

What to do next

Use the provider gateway to create an uplink to the external network.

Add an IP Space Uplink To a Provider Gateway in Your VMware Cloud Director

You can associate IP spaces to a provider gateway by creating IP space uplinks in VMware Cloud Director.

If the provider gateway for which you create the IP space uplink is private, i.e. dedicated to an organization, or if an organization has an edge gateway that is associated with the provider gateway, by creating the IP space uplink, you grant this organization access to the IP space with which the uplink is associated.

You can associate only one IP space with an IP space uplink. You cannot associate a private IP space to a public provider gateway.

Prerequisites

- Verify that your provider gateway is using IP spaces.
- Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Under Configure, click **IP Space Uplinks**.

4 Click **New**.

5 Enter the tenant facing name and optionally, a description for the IP space uplink, and click **Next**.

6 Select an IP space to associate with the IP space uplink and click **Next**.

7 (Optional) Select interfaces to map to the IP space uplink.

You can associate only some of the interfaces of the provider gateway to the uplink if you plan to create specific NAT rules to be applied only to the selected interfaces.

If necessary, you can edit the list of associated interfaces later.

8 Review your settings and click **Finish**.

Migrate a Provider Gateway to Using IP Spaces in Your VMware Cloud Director

Starting with VMware Cloud Director 10.5, you can migrate provider gateways from using IP blocks to using IP spaces.

When you prepare to migrate a provider gateway to using IP spaces, you must ensure that all existing IP blocks and static IP pools that are defined on the provider gateway are mapped to IP spaces. After setting up the IP spaces, you associate them to the gateway by creating an IP space uplink. To migrate IP prefixes, you must set up the IP prefixes sequences before starting the migration.

When you start the migration, VMware Cloud Director generates a violation report demonstrating if there are any mapping gaps that can cause the migration to fail.

One to one mappings of IP ranges are not strictly necessary for a successful migration. If a static IP pool was never used for allocating IP addresses, you can leave it out the IP space. However, the IP ranges that you configure as part of the preparation to migrate to IP spaces must match all IP addresses that are allocated from the provider gateway to its attached edge gateways, or the migration fails.

Note During the migration, VMware Cloud Director migrates only IP ranges that are mapped to the IP space uplinks on the provider gateway. This means that if any of the IP addresses on the edge gateway or the routed VDC networks associated with the provider gateway match with some private IP space within the organization, these edge gateway and networks IP addresses won't be migrated as part of the provider gateway migration.

VMware Cloud Director will try to migrate such IP addresses or networks only when you attempt to edit or update them. When you do this, this IP address or prefix gets marked as in-use, which results in a block of attempted updates by any other network or service that uses the same IP address or prefix. In this case, all the services and networks that are utilizing those duplicate IP addresses would continue to work without interruption.

Prerequisites

1. Verify that your role includes the **Provider Network:Edit** and **IP Spaces: Manage System** rights.
2. Create one or more IP spaces with scopes that cover all the IP blocks and static IP pools defined on the provider gateway and allocated to its attached edge gateways. To create the correct mappings, check the gateway's IP allocations and use those to define the necessary ranges and subnets. See Managing IP Spaces in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. Add an IP space uplink to the provider gateway that you want to migrate to IP spaces.
   a. From the top navigation bar, select **Resources** and click **Cloud Resources**.
   b. In the left pane, click **Provider Gateways**.
   c. Under Configure, click **IP Space Migration Prep**.
   d. Click **New**.
   e. Enter a tenant-facing name for the uplink.

   f Select the IP space that you created for the uplink and click **Next**.

   g Click **Finish**.

2 Click **Migrate to IP Spaces** and follow the prompts. Depending on the results of the static IP pools and network subnet violations checks, choose one of the options.

Option	Description
No Violations	Follow the prompts and finish the migration.
Static IP Pool Violations	a Cancel the migration wizard. b Edit the IP space that you created for the provider gateway to include the all IP addresses and ranges that are allocated to the provider gateway and are listed in violation. c Attempt the migration again.
Network Subnet Violations	a Cancel the migration wizard. b Edit the IP space that you created for the provider gateway to include all IP prefixes that are allocated to the provider gateway and are listed in violation. c Attempt the migration again.

Example: Mapping IP Blocks and Static IP Pools to IP Spaces

The following is an example of how to map the following defined IP blocks and static IP pools on an existing provider gateway to IP spaces.

IP Block	Static IP Pools	Local Usage of IPs
5.5.0.0/24	5.5.0.1-5.5.0.10, 5.5.0.20-5.5.0.40, 5.5.0.100-5.5.0.200	Internet
172.10.0.0/16	172.10.10.1-172.10.10.100	WAN
10.10.10.0/24	10.10.10.2-10.10.10.3, 10.10.10.100	Backup and other services

These three IP blocks logically map to three IP spaces to define as follows.

Name	Description	Type	Range	IP Prefix Sequence	Internal IP Scope
Internet	IP addresses to be used for accessing the internet	Public	5.5.0.1-5.5.0.10, 5.5.0.20-5.5.0.40	-	5.5.0.0/24
WAN	IP addresses to be used for accessing your corporate WAN	Private	172.10.10.1-172.10.10.100	-	172.10.0.0/24
Services	IP addresses to be used for service communication	Shared	10.10.10.2-10.10.10.3	-	10.10.10.0/29

Note

- For the Internet IP space, the Static IP pool range 5.5.0.100-5.5.0.200 was not used for any IP allocations, so the provider left it out of the new IP space range. There are no networks using this IP Space so no IP prefix sequence was defined. To not include this range in the IP space, the provider must first remove it from the IP block definition.
- For the WAN IP space, the scope was changed to be more narrow than what was defined in the IP block.
- For the services IP Space, only one of the Static Pools ranges were used to define the IP space range and the scope was reduced.

Autoconfigure BGP on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can autoconfigure BGP on your provider gateway.

Autoconfiguring BGP on a provider gateway generates a BGP neighbor, prefix list and route map based on the IP space uplink that you select.

Important If you choose to run autoconfigure again for the same IP space uplink, this resets the created BGP components to their default behavior.

Prerequisites

- Verify that your provider gateway uses IP spaces.
- Verify that you have the **System IP Spaces: View** and **Provider Gateway Routing: Manage** rights assigned to you.
- Verify that you associated at least one IP space to the provider gateway. See Add an IP Space Uplink To a Provider Gateway in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 On the right of the provider gateway name, click **Autoconfigure > BGP**.

5 (Optional) Enter the name of a BGP permission group to use for the autoconfiguration.

   If you don't enter a name, no BGP permission group is created as part of the configuration.

6 From the drop-down list, select an IP space uplink.

7 (Optional) To configure a BGP neighbor, enter an IPv4 or IPv6 address for the BGP neighbor.

8 If you entered and IP address for the BGP neighbor, enter a remote autonomous system (AS) ID number either in ASPLAIN or in ASDOT format.

9 Click **Autoconfigure**.

Autoconfigure Default NAT and Firewall Rules on a Provider Gateway in Your VMware Cloud Director

If you are using IP spaces, you can generate default SNAT, NO SNAT, and firewall rules on provider gateways in your VMware Cloud Director environment.

VMware Cloud Director autoconfigures the SNAT, NO SNAT, and firewall rules depending on the topology of the relevant IP spaces and their external and internal scopes.

There are some differences in the way autoconfiguration works for the different VMware Cloud Director versions.

Version	Behavior
VMware Cloud Director 10.5	If you associate a new IP space uplink with a provider gateway or if you reconfigure a specific IP space after you have autoconfigured NAT and firewall rules on a provider gateway, the gateway is not updated automatically with the changes. This means you must navigate to the gateway, delete all autoconfigured NAT and firewall rules and generate them again for each new IP space update.
VMware Cloud Director 10.5.1 and later	Rerunning autoconfiguration deletes all previously created NAT and firewall rules and recreates them. This includes the rules that were modified by users. All existing IP uplinks are taken into account during the reautoconfiguration.

Rules are applied in specific order.

Rule Type	Priority Order
NAT rules	■ Default NO SNAT rules are defined with a priority of 0, meaning the highest priority. The exception to this would be for an IP space where the external scope is the default route (i.e. 0.0.0.0/0). The NO SNAT rule associated with the default route has a priority of 1000. ■ Default SNAT rules have a priority of 100, again, with the exception of the SNAT rule associated with the default route. The SNAT rule associated with the default route has a priority of 1001. ■ User-created NAT rules have a priority of 50 by default.
Firewall rules	The order in which firewall rules are applied differs depending on your VMware Cloud Director version. In VMware Cloud Director 10.5.0, the rules are aplied as follows. 1 Firewall rules for associated default NO SNAT rules. 2 Firewall rules for associated default SNAT rules. 3 Existing firewall rules. In VMware Cloud Director 10.5.1, the rules are applied in the following order. 1 Firewall rules for associated default SNAT rules. 2 Firewall rules for associated default NO SNAT rules. 3 Existing firewall rules.

Default SNAT rule

This rule indicates that all traffic can access the external scope of a specific IP space by using NAT. The autoconfigured source is any IP address or CIDR, and the autoconfigured destination is the external scope of the IP space.

Default NO SNAT Rule

A NO SNAT rule allows traffic to flow from the IP space internal scope to its external scope without NAT rules being applied.

Associated Firewall Rule

An associated firewall rule is created for each default SNAT and NO SNAT rule.

Prerequisites

- Verify that you are a **system administrator** or that your role includes the **IP Spaces Default Gateway Services: Manage** right.
- Verify that the provider gateway is backed by an NSX tier-0 VRF gateway configured with active-standby high availability mode.
- Verify that the provider gateway is dedicated to a single tenant.
- Verify that you associated at least one IP space to the provider gateway. See Add an IP Space Uplink To a Provider Gateway in Your VMware Cloud Director.

- Verify that you configured the internal and external scopes for the IP spaces associated with the provider gateway.
- Verify that you configured the network topology for the IP spaces for which you want to autoconfigure NAT and firewall rules. See Configure the Network Topology For an IP Space in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 On the right of the provider gateway name, click **Autoconfigure > NAT and Firewall**.

4 Click **Autoconfigure**.

Configure Route Advertisement Topology Intentions on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, as a **service provider**, you can use the topology intentions feature to instruct VMware Cloud Director how to handle route advertisement within the network stack for each provider gateway.

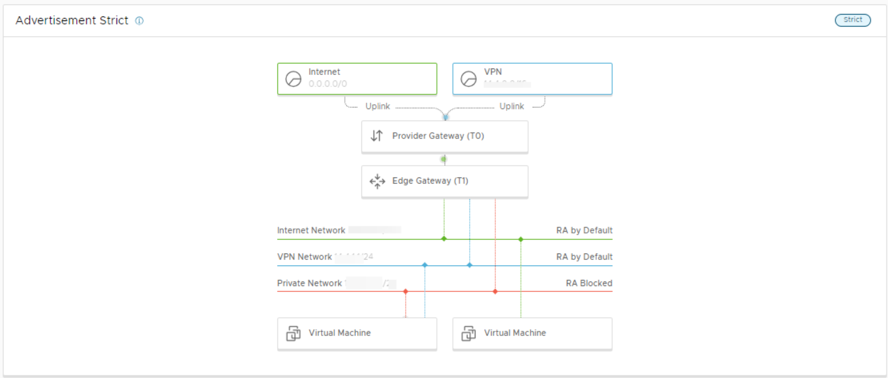
You configure your topology intentions on the provider gateway, and you can edit them later, if necessary.

Changing the provider gateway's topology intention settings does not affect any existing configuration components. However, if the topology intentions configuration includes specific restriction, for example, if you want only the IP spaces associated with an IP space uplink to be advertised, this setting will be enforced across the existing configuration.

To indicate your topology intent, you configure two types of settings - route advertisement intentions and NAT and firewall intentions.

Route Advertisement Intents

Intentions	Description
Advertisement Strict	This is the only available option for public provider gateways. In this topology configuration, every new routed network that is connected to an edge gateway which is backed by the provider gateway is automatically advertised if the network's subnet is a prefix from an IP space that is configured with an uplink on the provider gateway. You can turn off route advertisement for such networks manually, if necessary. For all other network, route advertisement is turned off and cannot be turned on.
Advertisement Flexible	Available to private provider gateways. In this topology configuration, only routed networks with IP spaces that are associated with an uplink are advertised by default. This can be changed on an individual network level later, if necessary. All other networks are not advertised by default but can be configured to be advertised after creation.
All Networks Advertised	Available to private provider gateways. In this topology, all networks are advertised by default from the edge gateway. This can be changed on an individual network level later, if necessary.



Prerequisites

- Verify that your provider gateway is private, i.e. that it is dedicated to a single organization. If a provider gateway is public, you can view it's topology configuration but you cannot edit it.
- Verify that your role includes the **Provider Network:Edit** right.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Under Topology Intentions, click **Route Advertisement**.

5 Click **Edit**.

6 Select one of the available options and click **Save**.

Configure NAT and Firewall Service Intentions on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, as a **service provider**, you can use the topology intentions feature to instruct VMware Cloud Director how to handle services configuration within the network stack for each provider gateway.

You configure your topology intentions on the provider gateway, and you can edit them later, if necessary.

Changing the provider gateway's topology intention settings does not affect any existing configuration components. However, if the topology intentions configuration includes specific restriction, for example, if you want only the IP spaces associated with an IP space uplink to be advertised, this setting will be enforced across the existing configuration.

To indicate your topology intent, you configure two types of settings - route advertisement intentions and NAT and firewall intentions.

NAT and Firewall Service Intentions

NAT and firewall service intentions indicate whether these services can be configured on edge gateways, on provider gateways, or both.

By default, NAT and firewall are configurable only on edge gateways.

Intention	Description
Provider Gateways	NAT and firewall are managed only on the provider gateways.
Edge Gateways	This is the only available option for public provider gateways. NAT and firewall rules are managed only on edge gateways.
Provider and Edge Gateways	NAT and firewall rules are configured both on provider gateways and edge gateways.

Prerequisites

- Verify that your provider gateway is private, i.e. that it is dedicated to a single organization. If a provider gateway is public, you can view it's topology configuration but you cannot edit it.
- Verify that your role includes the **Provider Network:Edit** right.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Under Topology Intentions, click **NAT and Firewall**.

5 Click **Edit**.

6 Select an option and click **Save**.

Configure Firewall Rules on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can configure firewall rules on your provider gateway that uses IP spaces.

Prerequisites

- Verify that the provider gateway is using IP spaces.
- Verify that the provider gateway is private, i.e. that it is dedicated to a single orgnization.
- Verify that the **NAT and Firewall Service Intentions** of the provider gateway is set to **Provider Gateways** or to **Provider and Edge Gateways**.
- Verify that your role includes the **Provider Gateway Firewall: View** and **Provider Gateway Firewall: Manage** rights.
- Verify that the backing NSX tier-0 router is in active-standby mode. Otherwise, you won't be able to set the **NAT and Firewall Service Intentions** of the provider gateway to **Provider Gateways** or to **Provider and Edge Gateways**.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Under Services, click **Firewall**.

5 To create a new firewall rule, click **New**.

6 Configure the firewall rule.

Name	Enter a name for the rule.
State	To enable the rule upon creation, turn on the **State** toggle.
Applications	(Optional) Choose one of the options. - To apply the rule to specific applications, turn on the **Applications** toggle, select the one or more applications from the list, and click **Save**. - To select specific ports to which the rule applies, click **Raw Port-Protocols**, select a protocol type, and enter source and destination ports or port ranges, separated by commas. You can add up to 15 port-protocol rows per rule.

Source	1 Choose one of the following options. ■ To allow or deny traffic from any source address, toggle on **Any Source**. ■ To allow or deny traffic from specific firewall groups, , click **Firewall Groups** and select the firewall groups from the list. ■ To enter IP addresses, CIDR blocks, or IP ranges manually, click **Firewall IP Addresses**, then click **Add** and enter the individual IP addresses, CIDR blocks, or ranges. 2 Click **Keep**.
Destination	1 Choose one of the following options. ■ To allow or deny traffic to any destination address, toggle on **Any Destination**. ■ To allow or deny traffic to specific firewall groups, click **Firewall Groups** and select the firewall groups from the list. ■ To enter IP addresses, CIDR blocks, or IP ranges manually, click **Firewall IP Addresses**, then click **Add** and enter the individual IP addresses, CIDR blocks, or ranges. 2 Click **Keep**.
Action	Select an option. ■ To allow traffic from or to the specified sources, destinations, and services, select **Allow**. ■ To block traffic from or to the specified sources, destinations, and services, without notifying the blocked client select **Drop**. ■ To block traffic from or to the specified sources, destinations, and services, and to notify the blocked client that traffic was rejected, select **Reject**.
IP Protocol	Select whether to apply the rule to IPv4, IPv6 traffic, or both.
Applied To	(Optional) From the drop-down menu, select an IP space uplink to which to apply the rule.
Logging	To have the address translation performed by this rule logged, turn on the **Logging** toggle. After you create the rule, in the Logging ID text box, you can see the unique NSX firewall rule ID that the system generates upon the rule creation.
Comment	(Optional) Add a comment to the firewall rule.

7 Click **Save**.

8 To change the position of the firewall rule, select the rule, click **Move to**, and, from the drop-down menu, select a new position.

9 To configure additional rules, repeat these steps.

Results

After a firewall rule is created, it appears in the Firewall Rules list. You can move up, move down, edit, or delete the rule as needed.

Configure NAT Rules on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can configure NAT rules on your provider gateway that uses IP spaces.

Prerequisites

- Verify that you are a **system administrator** or that your role includes the **Provider Gateway NAT: View** and the **Provider Gateway NAT: Manage** rights.
- Verify that the provider gateway is using IP spaces.
- Verify that the provider gateway is private, which means that it is dedicated to a single orgnization.
- Verify that the backing NSX tier-0 router is in active-standby mode. Otherwise, you won't be able to set the **NAT and Firewall Service Intentions** of the provider gateway to **Provider Gateways** or to **Provider and Edge Gateways**.
- Verify that you configured the NAT and firewall topology intention for the provider gateway to **Provider Gateways** or to **Provider and Edge Gateways**. See Configure Route Advertisement Topology Intentions on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **Provider Gateways**.
3. Click the provider gateway.
4. Under Services, click **NAT**.
5. To add a NAT rule, click **New**.
6. Enter a name and, optionally, a description for the rule.

7 From the drop-down menu, select a NAT action and enter the required info.

Action	Description	Settings
SNAT	Translates a source IP address of outbound packets so that packets appear as originating from a different network.	1 Enter an external IP address or a CIDR notation. 2 (Optional) Enter an internal IP address or a CIDR notation. 3 Enter a destination IP address or CIDR notation. This field is only applicable for SNAT and NO SNAT rules. If you want the rule to apply only for traffic to a specific domain, enter an IP address for this domain or an IP address list. If you leave this text box blank, the rule applies to all destinations outside of the local subnet.
NO SNAT	Turn off source NAT.	1 Enter an external IP address or a CIDR notation. 2 (Optional) Enter a destination IP address or CIDR notation.
DNAT	Translates the destination IP address of inbound packets so that packets are delivered to a target address into another network.	1 Enter an internal IP address or a CIDR notation. 2 (Optional) Enter an external port. 3 Enter an internal IP address or a CIDR notation. 4 From the drop-down menu, 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.
NO DNAT	Turn off destination NAT.	1 Enter an external IP address or a CIDR notation. 2 (Optional) Enter an external port.
Reflexive	Translates addresses passing through a routing device. Inbound packets undergo destination address rewriting, and outbound packets undergo source address rewriting.	1 Enter an external IP address or a CIDR notation. 2 Enter an internal IP address or a CIDR notation.

8 (Optional) Click **Advanced Settings**.

a To disable the rule upon creation, toggle off the **State** option.

This option is enabled by default.

b To enable logging, toggle on the **Logging** option.

c Enter a number to indicate the rule priority.

If multiple NAT rules exist for the same IP address, the rule with the highest priority is applied to it. A lower value means a higher precedence for this rule.

d From the drop-down menu, select how to expose the traffic that is subject to the NAT rule to the provider gateway firewall.

Option	Description
Match Internal Address	Apply the firewall to the internal address of the NAT rule. For SNAT, the internal address is the original source address before NAT is done. For DNAT, the internal address is the translated destination address after NAT is done.
Match External Address	Apply the firewall to the external address of the NAT rule. For SNAT, the external address is the translated source address after NAT is done. For DNAT, the external address is the original destination address before NAT is done.
Bypass	Bypass the firewall.

e From the drop-down menu, select an IP space uplink to which to apply the rule.

Note If you haven't associated any of the provider gateway interfaces to the IP space uplink that you select, the NAT rule applies to all of the provider gateway interfaces.

9 Click **Save**.

Configure BGP on a Provider Gateway That Uses IP Spaces in the VMware Cloud Director Service Provider Admin Portal

If you are using IP spaces on a provider gateway, you can configure a Border Gateway Protocol (BGP) connection on the provider gateway.

The set of capabilities that you can configure includes BGP route maps and BGP communities, which means that you can specify additional configuration for route redistribution. You can configure route maps with IP prefixes and community lists that are defined on the provider gateway.

In a provider gateway that is backed by a VRF gateway, graceful restart settings are read-only. You can edit these settings on the parent tier-0 in NSX.

If you are using NSX 4.1 or a newer version, you can edit the the local AS number on an provider gateway that is backed by a VRF gateway. In earlier versions, the local AS number setting is read-only and can be configured by a **system administrator** on the parent tier-0 in NSX.

Prerequisites

- Verify that your provider gateway uses IP spaces.
- Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **Provider Gateways**.
3. Click **BGP** and, under **Configuration**, click **Edit**.
4. Toggle on the **Status** option to enable BGP.
5. Enter an autonomous system (AS) ID number to use for the local AS feature of the protocol.

   VMware Cloud Director assigns the local AS number to the provider gateway. The provider gateway advertises this ID when it connects with its BGP neighbors in other autonomous systems.
6. From the drop-down menu, select a **Graceful Restart Mode** option.

Option	Description
Helper and graceful restart	It is not a best practice to enable the graceful restart capability on the provider gateway because the BGP peerings from all gateways are always active. In case of a failover, the graceful restart capability increases the time a remote neighbor takes to select an alternate tier-0 gateway. This delays BFD-based convergence. **Note** The provider gateway configuration applies to all BGP neighbors unless the neighbor-specific configuration overrides it.
Helper only	Useful for reducing or eliminating the disruption of traffic associated with routes learned from a neighbor that is capable of graceful restart. The neighbor must be able to preserve its forwarding table while it undergoes a restart.
Disable	Deactivate graceful restart mode on the edge gateway.

7. (Optional) Change the default value for the graceful restart timer.
8. (Optional) Change the default value for the stale route timer.
9. Toggle on the **ECMP** option to enable ECMP.
10. Click **Save**.

Add a BGP Neighbor On Your Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

You can configure individual settings for the BGP routing neighbors when you add them on the provider gateway.

Prerequisites

- Verify that you configured the global BGP settings for the provider gateway.
- Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Click **BGP** and click **Neighbors**.

5 Click **New**.

6 Enter the general settings for the new BGP neighbor.

   a Enter an IPv4 or IPv6 address for the new BGP neighbor.

   b Enter a remote Autonomous System (AS) number in ASPLAIN format.

   c Enter a time interval between sending keep-alive messages to a BGP peer.

   d Enter a time interval before declaring a BGP peer dead.

   e From the drop-down menu, select a **Graceful Restart Mode** option for this neighbor.

Option	Description
Disable	Overrides the global provider gateway settings and deactivates graceful restart mode for this neighbor.
Helper only	Overrides the global provider gateway settings and configures graceful restart mode as **Helper only** for this neighbor.
Graceful restart and Helper	Overrides the global provider gateway settings and configures graceful restart mode as **Graceful restart and Helper** for this neighbor.

   f Turn on the **AllowAS-in** toggle to enable receiving routes with the same AS.

   g If the BGP neighbor requires authentication, enter the password for the BGP neighbor.

7 Configure the Bidirectional Forwarding Detection (BFD) settings for the new BGP neighbor.

   a (Optional) Toggle on the **BFD** option to enable BFD for failure detection.

   b In the BDF interval text box, define the time interval for sending heartbeat packets.

   c In the **Dead Multiple** text box, enter the number of times the BGP neighbor can fail to send heartbeat packets before the BFD declares it is down.

8 Configure route filtering.

   a Select an IP address family from the **IP Address Family** drop-down menu.

   b Configure an inbound filter.

      1 Click **Set**.

      2 Toggle on the **Use Filter** option

      3 Select **Prefix List** or **Route Map** as filter type.

      4 Select one or more route maps or prefix lists from the list.

   c Configure an outbound filter.

      1 Click **Set**.

      2 Toggle on the **Use Filter** option.

      3 Select **Prefix List** or **Route Map** as filter type.

      4 Select one or more route maps or prefix lists from the list.

9 Click **Save**.

Configure an IP Prefix List on Your Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

You can create IP prefix lists which contain single or multiple IP addresses. You use IP prefix lists to assign BGP neighbors with access permissions for route advertisement.

The IP prefix lists are referenced through BGP neighbor filters to limit the number of BGP updates that are exchanged between BGP peers. By using route filtering, you can reduce the amount of system resources needed for BGP updates.

For example, you can add the IP address 192.168.100.3/27 to the IP prefix list and deny the route from being redistributed to the provider gateway.

You can also append an IP address with `less than or equal to` (le) and `greater than or equal to` (ge) modifiers to grant or limit route redistribution. For example, 192.168.100.3/27 ge 26 le 32 modifiers match subnet masks greater than or equal to 26-bits and less than or equal to 32-bits in length.

Prerequisites

Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Click **BGP** and click **IP Prefix Lists**.

5 To add a list, click **New**.

6 Enter a name and, optionally, a description for the prefix list.

7 Click **New** and add a CIDR notation for the prefix.

8 From the drop-down menu, select an action to apply to the prefix.

9 (Optional) Enter `greater than or equal to` and `less than or equal to` modifiers to grant or limit route redistribution.

10 Click **Save**.

What to do next

You can move the IP prefix list up or down the list, edit, or delete it.

Configure Community Lists on Your Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

You can create BGP community lists to define route maps based on the community lists.

A BGP community is a group of BGP routes that are labeled with extra information. This allows routers to better classify and handle routes that are sharing common attributes.

BGP community lists are user-defined lists of community attribute values. These lists can be used for matching or manipulating the communities attribute in BGP update messages.

BGP Communities attribute (RFC 1997) and the BGP Large Communities attribute (RFC 8092) are supported. The BGP Communities attribute is a 32-bit value split into two 16-bit values. The BGP Large Communities attribute has 3 components, each 4 octets in length.

In route maps, you can match on or set the BGP Communities or Large Communities attribute. You can use communities lists to enforce network policy based on the BGP community attributes.

Prerequisites

Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Click **BGP** and click **Communities Lists**

5 To add a communities list, click **New**.

6 Enter a name for the list.

7 Select a type of communities.

   Regular and large communities attributes are supported.

8 Specify a list of communities.

   If you are adding a regular community, you can select one or more of the well-known regular communities from the drop-down list.

   - NO_EXPORT - Do not advertise any of the routes received carrying a communities attribute that contains this value outside of the BGP confederation.
   - NO_ADVERTISE - Do not advertise any of the routes received carrying a communities attribute that contains this value to any BGP peer.
   - NO_EXPORT_SUBCONFED - Do not advertise any of the routes received carrying a communities attribute that contains this value to external BGP peers.

9 Click **Save**.

What to do next

Configure Route Maps on Your Provider Gateway.

Configure BGP Route Maps on Your Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

You can use route maps to define route policies at the BGP neighbor level and for route redistribution.

You create BGP route maps by defining a sequence of IP prefix lists, BGP path attributes, and an associated action.

When you use BGP route maps, the provider gateway scans the route or the traffic to which the criteria should be applied for a match, and if there is one, the router performs the action that you configured and stops scanning.

Prerequisites

- Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.
- Verify that you configured an IP prefix list or a community list.
- For details about using regular expressions to define route-map match criteria for community lists, see *Using Regular Expressions to Match Community Lists When Adding Route Maps* in the *NSX Administration Guide*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Provider Gateways**.

3 Click the provider gateway.

4 Click **BGP** and click **Route Maps**

5 To add a route map, click **New**.

6. Enter a name and, optionally, a description for the route map.
7. Click **New**.
8. From the drop-down menu, select a type of match criteria.
9.
10. Depending on the type of match criteria that you selected, choose one of the options.

Option	Description
IP Prefix	Click **Select IP prefix lists**, select the IP prefix lists from the list, and click **Save**.
Community List	a Click **Select Members and Match Criteria**. b Click **New**. c In the Match Expression column, specify match expressions that define how to match members of community lists. For each community list, the following match options are available: ■ **Match Any** - perform the set action in the route map if any of the communities in the community list is matched. ■ **Match All**- perform the set action in the route map if all the communities in the community list are matched regardless of the order. ■ **Match Exact**- perform the set action in the route map if all the communities in the community list are matched in the exact same order. ■ **Match Community Regex**- perform the set action in the route map if all the regular communities match the regular expression. ■ **Match Large Community Regex**- perform the set action in the route map if all the large communities match the regular expression. If you want to permit routes containing either the standard community or large community value, you must create two match criteria. If the match expressions are given in the same match criterion, only the routes containing both the standard and large communities will be permitted. For any match criterion, the match expressions are applied in an AND operation, which means that all match expressions must be satisfied for a match to occur. If there are multiple match criteria, they are applied in an OR operation, which means that a match will occur if any one match criterion is satisfied. d Enter an expression to match the community list and click **Save**.

11. In the Action column, select **Permit** or **Deny**.

    By selecting an action, you permit or deny IP addresses matched by the IP prefix or community lists to be advertised.

12 Configure BGP attributes.

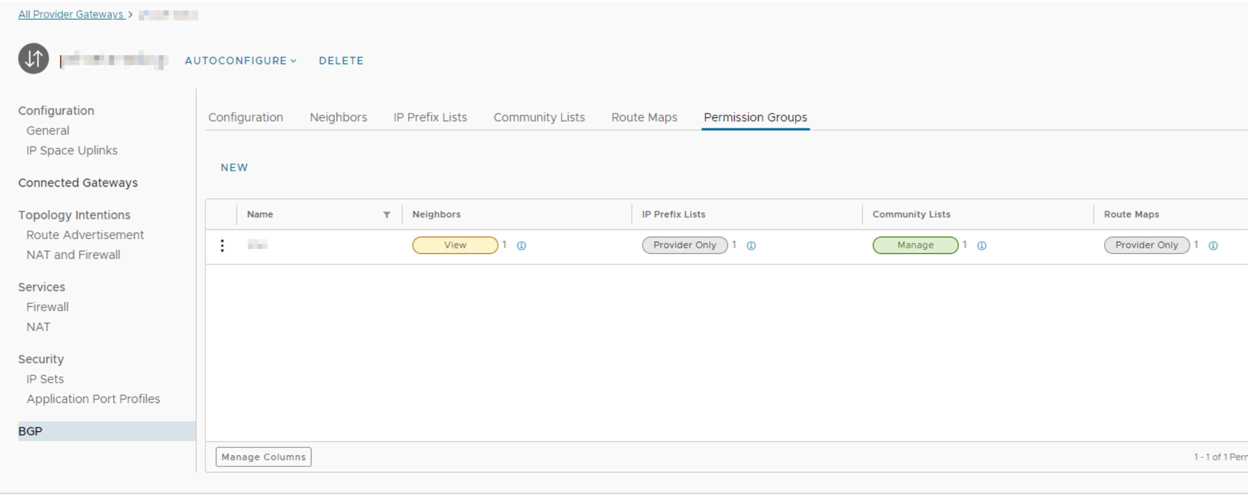
Option	Description
Weight	Enter a weight value to influence path selection. The range is 0 - 65535.
Local Preference	Use this value to choose the outbound external BGP path. The path with the highest value is preferred.
Path Prepend	Prepend a path with one or more autonomous system numbers to make the path longer and therefore less preferred.
Prefer global IPv6	To opt for IPv6 path selection, turn on the **Prefer global IPv6** option.
Multi Exit Discriminator	Multi-exit discriminator indicates to an external peer a preferred path to an autonomous system.
Community	Specify a list of communities. For a regular community use the aa:nn format, for example, 300:500. For a large community use the aa:bb:cc format, for example, 11:22:33. You can select one or more of the well-known regular communities from the drop-down list. ■ NO_EXPORT_SUBCONFED - Do not advertise to external BGP peers. ■ NO_ADVERTISE - Do not advertise to any peer. ■ NO_EXPORT - Do not advertise outside BGP confederation.

13 Click **Save**.

Configure A BGP Permission Group on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can manage tenant access to BGP configuration settings on your provider gateways.

You can assign different tenant permissions for the four BGP configuration items. There are three levels of access that you can assign for each of these items - **Provider Only**, **View**, or **Manage**. After creating a permissions group for a specific organization, you can edit the permissions that you assigned as necessary.



All Provider Gateways > [redacted]

[redacted] AUTOCONFIGURE DELETE

	Name	Neighbors	IP Prefix Lists	Community Lists	Route Maps
⋮	[redacted]	View 1 ⓘ	Provider Only 1 ⓘ	Manage 1 ⓘ	Provider Only 1 ⓘ

Note For a tenant user to view and manage BGP components, their role must include the **Limited Provider Gateway BGP: View** and the **Limited Provider Gateway BGP: Manage** rights.

Prerequisites

- Verify that you have the **Provider Gateway Routing: View** and **Provider Gateway Routing: Manage** rights assigned to you.
- Verify that the provider gateway is using IP spaces.
- Verify that the provider gateway is private (dedicated to a single organization).

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **Provider Gateways**.
3. Click the provider gateway.
4. Click **BGP** and click **Permission Groups**.
5. Click **New**.
6. Enter a name and, optionally, a description for the permissions group.
7. From the drop-down menu for each of the 4 BGP components, select the level of access that you want to provide to the organization.

   The default permission setting for each component is **Provider Only**, which provides no tenant access to BGP configuration settings.

   You can choose different permission settings for the different BGP components.

   - If you don't want to prevent any tenant access to the component, leave the **Provider Only** selection.
   - If you want to grant the organization a permission to view the component, select **View**.

- If you want to grant the organization a permission to edit the settings for the componet, select **Manage**.

8 Click **Save**.

What to do next

If necessary, you can edit the BGP permissions for each component of the permissions group.

Managing IP Spaces in the VMware Cloud Director Service Provider Admin Portal

You can use **IP Spaces** to manage your IP address allocation needs. **IP Spaces** provide a structured approach to allocating public and private IP addresses by preventing the use of overlapping IP addresses across organizations and organization VDCs.

An IP space consists of a set of defined non-overlapping IP ranges and small CIDR blocks that are reserved and used during the consumption aspect of the IP space life cycle. An IP space can be either IPv4 or IPv6, but not both.

Every IP space has an internal scope and an external scope. The internal scope of an IP space is a list of CIDR notations that defines the exact span of IP addresses in which all ranges and blocks must be contained in. The external scope defines the total span of IP addresses to which the IP space has access, for example, the internet or a WAN. The internal and external scopes are used to define default NAT rules and BGP prefixes.

As a **service provider**, you create public, shared, or private IP spaces and assign them to provider gateways by creating IP space uplinks. After creating an IP space, you can assign to it IP prefixes for networks and floating IP addresses for network services.

Organization administrators can view general information about the IP spaces in their organization has access, and manage the IP spaces available to them.

There are three types of IP spaces that you can create.

Public IP Space

A public IP space is used by multiple organizations and is controlled by the **service provider** through a quota-based system.

Shared IP Space

An IP space for services and management networks that are required in the tenant space, but as a **service provider**, you don't want to expose it to organizations in your environment.

Private IP Space

Private IP spaces are dedicated to a single tenant - a private IP space is used by only one organization that is specified during the space creation. For this organization, IP consumption is unlimited.

Add a Public IP Space to Your VMware Cloud Director

You can create a public IP space to be used by multiple VMware Cloud Director organizations and control it through a quota system.

As a **service provider**, you can add an public IP space that can be used by a number of organizations. Tenant consumption of IP addresses is based on a set quota of non-overlapping IP ranges and CIRD blocks that you define.

An IP Space can be either IPv4 or IPv6, but not both.

Prerequisites

Verify that your role includes the **System IP Spaces:View** and **System IP Spaces:Manage** rights.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **IP Spaces** and click **New**.
3. If you are using a multisite deployment, select a site where to create the IP space from the drop-down list.
4. In the IP space **Type** page, select **Public** and click **Next**.
5. Enter a name and, optionally, a description for the new IP space, and click **Next**.
6. (Optional) On the Network Topology page, toggle on the route advertisement option to enable advertising networks with IP prefixes from this IP space.
7. (Optional) If you want to autogenerate default NAT rules, in the Default Autoconfiguration Rules section, select the relevant check boxes.

Default Autoconfiguration Rule	Description
SNAT rule	The default SNAT rule source is ANY and the destination is the external scope of the IP space.
NO SNAT rule	The default NO SNAT rule source is the internal scope of the IP space and its destination is the external scope of the IP space.
Matching Firewall rule	A default firewall rulew is created for any corresponding default NAT rule.

8. Click **Next**.
9. To define the IP space scope, enter up to five IP ranges and prefixes.

   The internal scope of an IP space is a list of CIDR notations that defines the exact span of IP adresses in which all ranges and blocks must be contained in. The internal scope of the IP space is used to define default NAT rules and BGP prefixes.

   You can use either IPv4 or IPv6.

10 (Optional) Enter a CIDR notation for the external scope for the IP space.

   The external scope defines the total span of IP addresses to which the IP space has access, for example the internet or a WAN. The external scope of the IP space is used to define default NAT rules and BGP prefixes.

11 Click **Next**.

12 (Optional) Enter IP ranges for the IP space and click **Next**.

13 (Optional) Enter IP prefixes for the IP space and click **Next**.

14 If you entered at least one floating IP address in the IP Ranges page, enter a number of floating IP addresses to allocate individually or select the **Unlimited** checkbox.

15 If you entered at least one IP prefix in the IP Prefixes page, enter a number of IP prefixes, or select the **Unlimited** checkbox, and click **Next**.

16 Review the **Ready to Complete** page, and click **Finish**.

Add a Shared IP Space to Your VMware Cloud Director

You can add a shared IP space to use for multiple VMware Cloud Director organizations.

You can use an IP space for services and management networks that are required in the tenant space but you don't want to expose to organizations in your environment.

Prerequisites

Verify that your role includes the **System IP Spaces:View** and **System IP Spaces:Manage** rights.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **IP Spaces** and click **New**.

3 If you are using a multisite deployment, select a site where to create the IP space from the drop-down list.

4 In the IP space **Type** page, select **Shared** and click **Next**.

5 Enter a name and, optionally, a description for the new IP space, and click **Next**.

6 (Optional) On the Network Topology page, toggle on the route advertisement option to enable advertising networks with IP prefixes from this IP space.

7 (Optional) If you want to autogenerate default NAT rules, in the Default Autoconfiguration Rules section, select the relevant check boxes.

Default Autoconfiguration Rule	Description
SNAT rule	The default SNAT rule source is ANY and the destination is the external scope of the IP space.
NO SNAT rule	The default NO SNAT rule source is the internal scope of the IP space and its destination is the external scope of the IP space.
Matching Firewall rule	A default firewall rulew is created for any corresponding default NAT rule.

8 To define the IP space scope, enter up to five IP ranges and prefixes.

The internal scope of an IP space is a list of CIDR notations that defines the exact span of IP adresses in which all ranges and blocks must be contained in. The internal scope of the IP space is used to define default NAT rules and BGP prefixes.

You can use either IPv4 or IPv6.

9 (Optional) Enter a CIDR notation for the external scope for the IP space.

The external scope defines the total span of IP addresses to which the IP space has access, for example the internet or a WAN. The external scope of the IP space is used to define default NAT rules and BGP prefixes.

10 Click **Next**.

11 (Optional) Enter IP ranges for the IP space and click **Next**.

12 If you entered at least one floating IP address in the IP Ranges page, enter a number of floating IP addresses to allocate individually or select the **Unlimited** checkbox.

13 If you entered at least one IP prefix in the IP Prefixes page, enter a number of IP prefixes, or select the **Unlimited** checkbox, and click **Next**.

14 Review the **Ready to Complete** page, and click **Finish**.

Add a Private IP Space to Your VMware Cloud Director

You can create an IP space to be used by a single VMware Cloud Director organization.

As a **service provider**, you can dedicate an IP space to a single organization. By default, the IP address quota for a private IP space is unlimited. **Organization administrators** and other users with the appropriate set of rights can allocate IP addresses from a private IP space.

Prerequisites

Verify that your role includes the **Private IP Spaces:View** and **Private IP Spaces:Manage** rights.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **IP Spaces** and click **New**.

3 If you are using a multisite deployment, select a site where to create the IP space from the drop-down list.

4 In the IP space **Type** page, select **Private**.

5 From the drop-down menu, select an organization to which to dedicate the IP space.

6 Click **Next**.

7 Enter a name and, optionally, a description for the new IP space, and click **Next**.

8 (Optional) On the Network Topology page, toggle on the route advertisement option to enable advertising networks with IP prefixes from this IP space.

9 (Optional) If you want to autogenerate default NAT rules, in the Default Autoconfiguration Rules section, select the relevant check boxes.

Default Autoconfiguration Rule	Description
SNAT rule	The default SNAT rule source is ANY and the destination is the external scope of the IP space.
NO SNAT rule	The default NO SNAT rule source is the internal scope of the IP space and its destination is the external scope of the IP space.
Matching Firewall rule	A default firewall rulew is created for any corresponding default NAT rule.

10 Click **Next**.

11 To define the IP space scope, enter up to five IP ranges and prefixes.

The internal scope of an IP space is a list of CIDR notations that defines the exact span of IP adresses in which all ranges and blocks must be contained in. The internal scope of the IP space is used to define default NAT rules and BGP prefixes.

You can use either IPv4 or IPv6.

12 (Optional) Enter a CIDR notation for the external scope for the IP space.

The external scope defines the total span of IP addresses to which the IP space has access, for example the internet or a WAN. The external scope of the IP space is used to define default NAT rules and BGP prefixes.

13 Click **Next**.

14 (Optional) Enter IP ranges for the IP space and click **Next**.

15 (Optional) Enter IP prefixes for the IP space and click **Next**.

16 If you entered at least one floating IP address in the IP Ranges page, enter a number of floating IP addresses to allocate individually or select the **Unlimited** checkbox.

17 If you entered at least one IP prefix in the IP Prefixes page, enter a number of IP prefixes, or select the **Unlimited** checkbox, and click **Next**.

18 Review the **Ready to Complete** page, and click **Finish**.

Edit an IP Space in Your VMware Cloud Director

In VMware Cloud Director, you can modify the name, description, scope, IP ranges, and IP prefixes of an existing IP space.

Prerequisites

Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **IP Spaces**.
3. Click the IP space that you want to edit.
4. Under General, click **Edit**.
5. Edit the IP Space name or description.
6. Edit the service scope of the IP Space.
   a. Click the **Service Scope** tab.
   b. Add up to five IP addresses for the internal scope of the IP space.
   c. Add an external scope for the IP space.
7. Edit the IP ranges of the IP space.
   a. Click the **IP Ranges** tab.
   b. Add up to five IP ranges that match the internal scope of the IP space.
8. Edit the IP prefixed of the IP space.
   a. Click the **IP Prefixes** tab.
   b. Edit the IP prefixes for the IP space.
9. Click **Save**.

Enable Route Advertisement For an IP Space in VMware Cloud Director

In VMware Cloud Director, you can enable route advertisement for the networks that are using an IP space.

You can enable route advertisment for the networks that are using a specific IP space to facilitate the creation of a fully routed environment in an organization. After enabling the route advertisement for an IP space, you can configure route advertisment for each network to advertise routes from the edge gateways to the provider gateways.

Prerequisites

Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **IP Spaces**.
3. Click the name of the IP space.
4. Under Configuration, click **Network Topology**.
5. Toggle on the **Route Advertisement** option.
6. Click **Save**.

What to do next

- Configure the route advertisement topology intentions for the provider gateway with which the IP space is associated. See Configure Route Advertisement Topology Intentions on a Provider Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Configure route advertisement for specific networks. See Add a Routed Organization Virtual Data Center Network in the *VMware Cloud Director Tenant Guide*.

Allocate Floating IP Addresses To an IP Space in Your VMware Cloud Director

In VMware Cloud Director, you can allocate IP addresses for individual use to an IP space.

Floating IP address ranges are simple ranges of IP addresses from which IP addresses are pulled out individually.

Prerequisites

- Verify that you have added at least one IP range in the IP space.
- Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left pane, click **IP Spaces**.
3. Click the name of the IP space to which you want to allocate floating IP addresses.
4. Click **Quota** and click **Edit**.
5. Choose one of the following.
   - Enter a number of floating IPs to allocate to the IP space.
   - Select the **Unlimited** check box.
6. Click **Save**.

Allocate IP Prefixes To an IP Space in Your VMware Cloud Director

In VMware Cloud Director, you can allocate IP prefixes to an IP space to be used for the configuration of networks.

An IP prefix block is defined by the starting block of the sequence - the IP prefix, and the number of IP prefix blocks in that sequence.

Prerequisites

Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **IP Spaces**.

3 Click the name of the IP space to which you want to allocate IP prefixes.

4 Click **General** and scroll down to the IP Prefixes section.

5 Click **Edit**.

6 Click **Add**.

7 Add the first IP address of the IP prefix sequence.

8 Enter a number of prefixes that you want to allocate.

9 Click **Save**.

Configure the Network Topology For an IP Space in Your VMware Cloud Director

To help enable north-south traffic within your VMware Cloud Director environment, you must configure the network topology for the IP spaces in it.

Prerequisites

- Verify that your role includes the **IP Spaces:View** and **IP Spaces:Configure** rights.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **IP Spaces**.

3 Click the name of the IP space and, under Configuration, click **Network Topology**.

4 Click **Edit**.

5 Select the **Route Advertisement Allowed** check box to enable route advertisement if routed networks associated with this IP Space need to be advertised from the edge gateway to the provider gateway.

6 Configure default autoconfiguration rules.

   To autogenerate default NAT rules, you must configure both the internal and the external scope of this IP space.

   a Select the check box to enable the creation of a default SNAT rule.

   b Select the check box to enable the creation of a default NO SNAT rule.

   c Select the check box to enable the creation of a matching firewall rule for each default NAT rule.

7 Click **Save**.

What to do next

You can now autoconfigure default NAT and associated firewall rules for this IP space on either the edge gateway or the provider gateway that are associated with it. See Autoconfigure Default NAT and Firewall Rules on a Provider Gateway in Your VMware Cloud Director and Autoconfigure NAT and Firewall Rules on an NSX Edge Gateway in VMware Cloud Director.

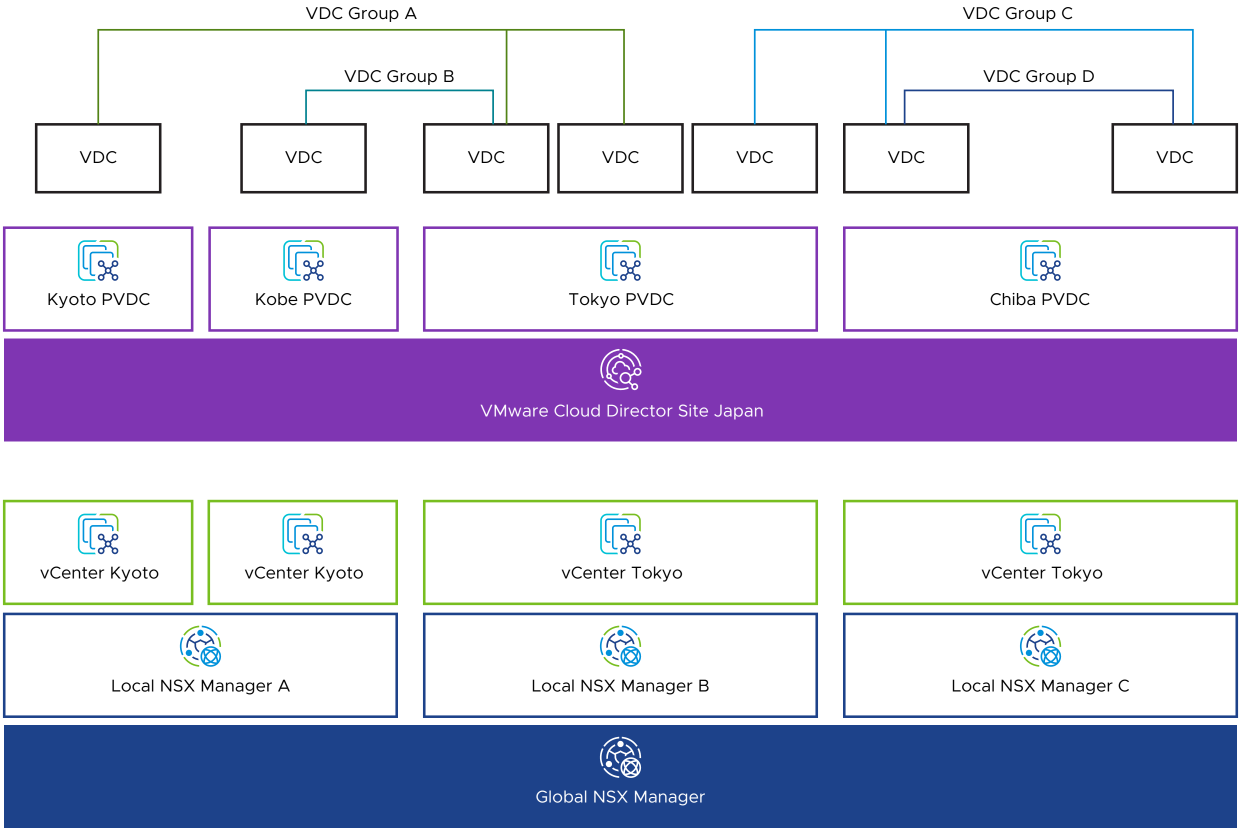
Managing NSX Federation in VMware Cloud Director

Starting with version 10.5, VMware Cloud Director supports NSX federation.

As a **service provider**, you can leverage the NSX federation functionality to create edge gateways and segments that span one or more NSX locations, configure and enforce firewall rules consistently, and manage networking and security across NSX Manager instances within your VMware Cloud Director environment through a single pane of glass view.

You can also enable tenants to configure and enforce firewall rules across NSX Manager instances.

When you use NSX federation, you can group together multiple NSX Manager instances in a universal NSX VDC group. Universal edge gateways and networks are separate from local edge gateways and networks. VDCs can be part of more than one group, and any vCenter Server instance can support multiple VDCs that are included in the same data center group.



Note In VMware Cloud Director 10.5, NSX federation for multisite deployments is not supported. This means that you can have multiple NSX Manager instances that are federated and manage them through a single global instance only if they are registered to the same VMware Cloud Director site.

Workflow

1 Familiarize yourself with the NSX Federation documentation. See Getting Started with NSX Federation in the *NSX Installation Guide* and NSX Federation in the *NSX Administration Guide*.

2 In NSX, install the Global Manager, configure the Global Manager as active, and add locations.

3 Register the global NSX Manager instance to VMware Cloud Director. See Register an NSX Manager Instance with VMware Cloud Director.

   The global NSX Manager instance details include all local NSX Manager instances that are under its domain. You can view the registered NSX location names in the VMware Cloud Director Service Provider UI.

   Note You must configure at least one edge cluster per location for each local NSX Manager instance.

4 Import a provider gateway that is associated with your global NSX Manager instance. See Add a Provider Gateway to Your VMware Cloud Director.

5 Configure custom segment profile templates in the global NSX Manager instance. See Segment Profiles in the *NSX Administration Guide* and Using NSX Manager Segment Profile Templates in VMware Cloud Director.

   When you create custom segment profiles and profile templates by using the global NSX Manager instance, they are synced across all NSX Manager instances in the federation.

Caveats and Limitations

There are some caveats and limitations to consider when using NSX federation with VMware Cloud Director.

- A data center group can be either local or global, and once you create it, it cannot be changed.
- NSX federation for multisite deployments is not supported. This means that you can have multiple NSX Manager instances that are federated and manage them through a single global instance only if they are registered to the same VMware Cloud Director site.
- You can include up to 4 NSX Manager instances in a data center group.
- Each NSX Manager supports up to 16 vCenter instances.
- The provider gateway that is associated with your global NSX Manager instance and with a data center group defines the boundaries of the data center group.
- NSX federation in VMware Cloud Director supports only routed data center networks. All data center group networks span the full scope of the egress point for the data center group.
- You can use global custom segment profile templates in global data center groups.
- VMware Cloud Director service does not support NSX federation.

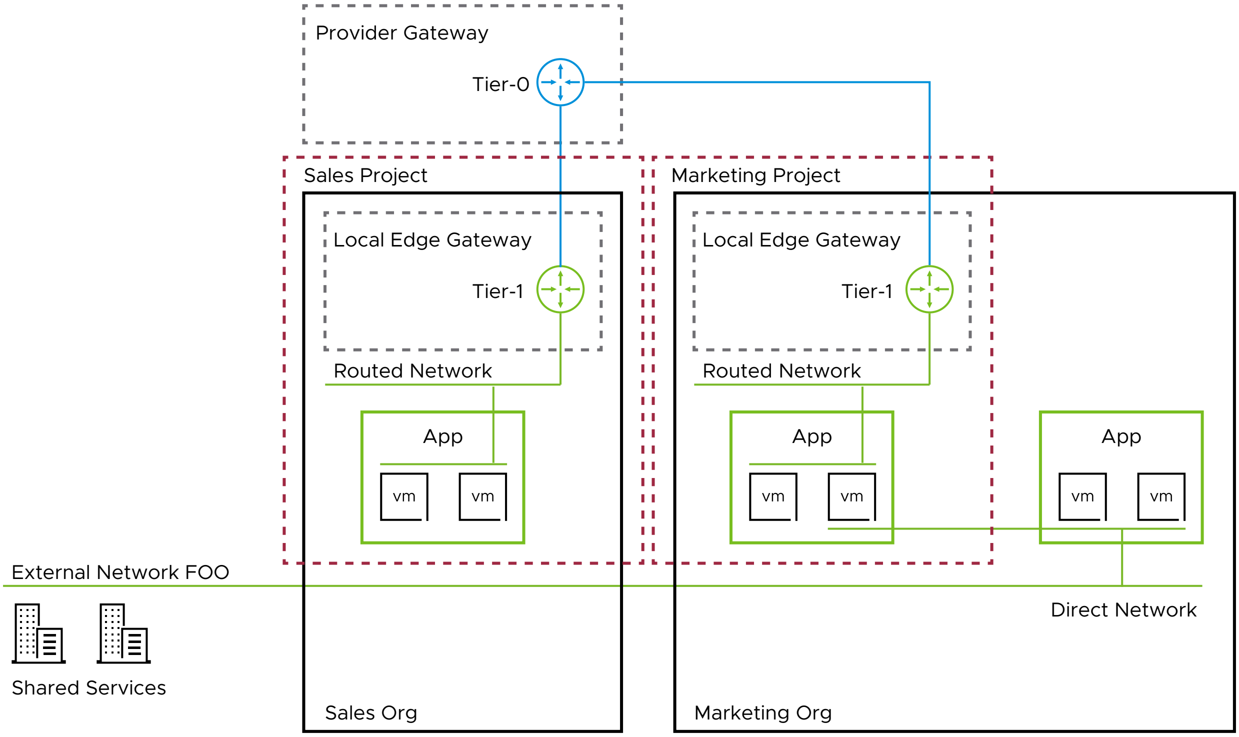
Managing NSX Tenancy in VMware Cloud Director Service Provider Admin Portal

Starting with version 10.5.1, VMware Cloud Director offers support for NSX multitenancy by mapping organizations directly to NSX projects.

You can learn more about NSX projects by familiarizing yourself with the relevant NSX Projects documentation in the *NSX Administration Guide*.

To use NSX tenancy in the context of VMware Cloud Director, begin by activating NSX tenancy for an organization.

After that, you can opt in or out of using NSX tenancy when you create VDCs in this organization. The NSX project is actually created during the creation of the first VDC in the organization for which you activated NSX tenancy. The name of the NSX project is the same as the name of the organization to which it is mapped.



In the diagram, the Sales and Marketing VMware Cloud Director organizations are mapped to the corresponding NSX projects. All NSX components created within the organization context are part of the NSX project. The provider (tier-0) gateway is associated to the NSX project but it is not part of it, providing connectivity to local edge gateways and to direct NSX networks, if necessary. An external network connection is available to the Marketing Org through a direct network. There are no restrictions on whether the backing segments for the imported and external networks are within the NSX project or not.

If you choose not to activate NSX tenancy during the creation of an organization VDC, you cannot change this setting later.

Some use cases do not require organization VDC participation in NSX tenancy, for example, if the VDC only needs VLAN networks. Additionally, organization VDCs using NSX tenancy are restricted to using the network pool that is backed by the default overlay transport zone, so, in order to be able to use a different network pool, you might wish to opt out of NSX tenancy.

If you opt into NSX tenancy during the creation of an organization VDC, you cannot change its network pool later. However, you may still add external network connections to edge gateways and create imported networks within the VDC.

You can deactivate NSX tenancy for an organization only after you delete all its affiliated VDCs and data center groups with active NSX tenancy.

Note When you enable NSX tenancy for an organization, any organization VDCs that you create after that have NSX tenancy enabled by default. For existing organization VDCs and VDC groups, NSX tenancy is not enabled.

Data Center Group Networking

When a tenant creates a data center group, if the starting VDC uses NSX tenancy, then the data center group will use NSX tenancy as well. The tenant can scope edge gateways to the data center group only if the edge gateways are also using NSX tenancy and if they belong to the same organization as the data center group.

Tenants can create data center groups that include both organization VDCs that are using NSX tenancy and VDCs that aren't using NSX tenancy.

In a multisite context, tenants can create data center groups that include organization VDCs from associated organizations. In this case, all networking and security components in the data center group remain within the NSX project of the starting organization VDC.

Because the NSX project is mapped to the organization of the starting VDC, in this kind of mixed data center groups, distributed firewall rules and security groups are all deployed within the context of the NSX project.

Note that associated organizations can have their own NSX, but these have no impact on the DC group networks. VMs and vApps can connect to these DC networks and to local networks that are not part of the project at the same time.

Caveats and Limitations

Not all VMware Cloud Director networking features are supported within the context of NSX tenancy. To learn more, see the full list of the Features Available for Consumption under NSX Projects.

Note VMware Cloud Director does not support using segment profiles within NSX tenancy.

Activate NSX Tenancy for an Organization in VMware Cloud Director Service Provider Admin Portal

To use NSX tenancy in the context of VMware Cloud Director, first you define the NSX project in VMware Cloud Director by activating NSX tenancy for an organization.

Prerequisites

- Verify that you configured a default overlay transport zone in NSX. See Create Transport Zones in the *NSX Installation Guide*
- Verify that you created a network pool that is backed by the default overlay transport zone that you created. See Geneve Network Pools in Your VMware Cloud Director.
- Verify that your role includes the **Organization: Edit Properties** right.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 From the left panel, select **Organizations**.

3 Click the name of the organization.

4 Under Networking, click **NSX Tenancy**.

5 Click **Edit**.

6 Toggle on the **Networking Tenancy** option.

7 (Optional) Enter a log name of up to eight characters for the NSX project.

   The log name is a globally unique identifier for the organization in the NSX logs.

8 Click **Save**.

What to do next

1 Create an Organization Virtual Data Center in VMware Cloud Director

2 To use vApp network services within the project, assign an edge cluster to the organization VDC that uses NSX tenancy. See Assign an Edge Cluster to a VMware Cloud Director Organization Virtual Data Center

3 Create an NSX edge gateway scoped to the organization VDC. See Add an Edge Gateway Backed by an NSX Provider Gateway in VMware Cloud Director.

Managing NSX Edge Gateways in VMware Cloud Director Service Provider Admin Portal

An NSX edge gateway provides a routed organization VDC network or a data center group network with connectivity to external networks and IP management properties. It can also provide services such as firewall, network address translation (NAT), IPSec VPN, DNS forwarding, and DHCP, which is enabled by default.

Add an Edge Gateway Backed by an NSX Provider Gateway in VMware Cloud Director

In VMware Cloud Director, an edge gateway backed by an NSX gateway provides a routed organization VDC network with services such as load balancing, network address translation, and firewall.

Prerequisites

For information about the system requirements for deploying an NSX edge gateway, see the *NSX Administration Guide*.

You can dedicate a provider gateway to an entire organization, which makes possible connecting multiple edge gateways to a dedicated provider gateway. See Managing Provider Gateways in Your VMware Cloud Director.

VMware Cloud Director supports basic NSX edge cluster configuration. For more information on NSX edge clusters, see *NSX Installation Guide*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click **New**.

4 Select the NSX-backed organization VDC on which you want to create the edge gateway, and click **Next**.

5 Enter a name and, optionally, a description for the new edge gateway.

6 To enable IP space management for the edge gateway, toggle on the **IP Address Management** option, and click **Next**.

7 To dedicate a provider gateway to the edge gateway, toggle on the **Dedicate Provider Gateway** option.

8 Select a provider gateway to which the new edge gateway connects and click **Next**.

9 Select an edge cluster on which to deploy the new edge gateway and click **Next**.

   If you want to run the edge gateway services on an edge cluster that is different from the one associated with the provider gateway, you can configure the edge gateway to use a different edge cluster.

   - Use the edge cluster of the external network to which the edge gateway is connected.
   - Select from a list of edge clusters available to the organization VDC on which you are deploying the edge gateway.

10 Review the **Ready to Complete** page, and click **Finish**.

Autoconfigure NAT and Firewall Rules on an NSX Edge Gateway in VMware Cloud Director

If you are using IP spaces, you can generate default SNAT, NO SNAT, and firewall rules on edge gateways in your environment.

VMware Cloud Director autoconfigures the SNAT, NO SNAT, and firewall rules depending on the topology of the relevant IP spaces and their external and internal scopes.

Rules are applied in specific order.

Rule Type	Priority Order
NAT rules	■ Default NO SNAT rules are defined with a priority of 0, meaning the highest priority. The exception to this would be for an IP space where the external scope is the default route (i.e. 0.0.0.0/0). The NO SNAT rule associated with the default route has a priority of 1000. ■ Default SNAT rules have a priority of 100, with the exception of the SNAT rule associated with the default route. The SNAT rule associated with the default route has a priority of 1001. ■ User-created NAT rules have a priority of 50 by default.
Firewall rules	Firewall rules are applied in the following order. 1 Firewall rules for associated default NO SNAT rules. 2 Firewall rules for associated default SNAT rules. 3 Existing firewall rules.

Default SNAT rule

This rule indicates that all traffic can access the external scope of a specific IP space by using NAT. The autoconfigured source is any IP address or CIDR, and the autoconfigured destination is the external scope of the IP space.

Default NO SNAT Rule

A NO SNAT rule allows traffic to flow from the IP space internal scope to its external scope without NAT rules being applied.

Associated Firewall Rule

Default firewall rules are autoconfigured only after SNAT or NO SNAT rules are successfully generated. An associated firewall rule is created for each default SNAT and NO SNAT rule.

Prerequisites

- Verify that you are a **system administrator** or that your role includes the **IP Spaces Default Gateway Services: Manage** right.
- Verify that the edge gateway is connected to a provider gateway that has at least one IP space uplink.
- Verify that you configured the internal and external scopes for the IP spaces associated with the provider gateway.
- Verify that you configured the network topology for the IP spaces for which you want to configure NAT and firewall rules. See Configure the Network Topology For an IP Space in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3. Click the edge gateway.
4. On the right of the edge gateway name, click **Autoconfigure NAT/FW**.
5. Review the IP spaces for which NAT and firewall rules will be generated and click **Autoconfigure**.

Add an External Network Connection to an NSX Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can configure external network connections to a NSX edge gateway, allowing tenants to configure static route scopes, NAT rules, and firewall rules to apply to a specific external network connection.

Starting with version 10.4.1, VMware Cloud Director supports configuring external network connections to NSX edge gateways.

As a **system administrator**, you can connect multiple external networks to a single edge gateway. After you set up your external network connections, an **organization administrator** can configure static route scopes, NAT rules, and firewall rules on the edge gateway to apply to a specific external network connection.

Note You can connect an external network that is backed by a VLAN segment only to one edge gateway.

Prerequisites

- Verify that the external network is backed by an NSX segment.
- Verify that the edge gateway that you want to configure is backed by NSX.
- Verify that you are a **system administrator**.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway.
4. Under Configuration, click **External Networks**.
5. Click **Connect New**.
6. From the drop-down, select an external network to which to create a connection.
7. Select a subnet.
8. Enter a number of IP addresses to be allocated from the selected subnet.
9. Select an assignment method for the IP address.

   If you select **Manual**, enter an IP address for the external network connection.
10. Click **Save**.

Add an IP Set to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

To create firewall rules and add them to an NSX edge gateway, you must first create IP sets. IP sets are groups of objects to which the firewall rules apply. Combining multiple objects into IP sets helps reduce the total number of firewall rules to be created.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway.
4. Under **Security**, click **IP Sets** tab and click **New**.
5. Enter a name and, optionally, a description for the IP set.
6. Enter an IP address or an IP addresses range for the virtual machines that the IP set includes, and click **Add**.
7. To save the firewall group, click **Save**.

Results

You created an IP set and added it to the NSX edge gateway.

What to do next

Add an NSX Edge Gateway Firewall Rule in the VMware Cloud Director Service Provider Admin Portal

Add an NSX Edge Gateway Firewall Rule in the VMware Cloud Director Service Provider Admin Portal

To control the incoming and outgoing network traffic to and from an NSX edge gateway, you create firewall rules.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the edge gateway.
4. If the **Firewall** screen is not already visible under the Services section, click the **Firewall** tab.
5. Click **New**.

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) Depending on your VMware Cloud Director version and your environment needs, the options vary. ■ You can select specific applications to which the rule applies. Click the pencil icon, select one or more applications from the list, and click **Save**. ■ If you are using VMware Cloud Director 10.5.1 or later, you can select specific ports to which the rule applies. Select the **Raw Port-Protocols** tab, click **Add**, select a protocol type, and enter source and destination ports or port ranges separated by commas. You can add up to 15 port-protocol rows per rule.
Context	(Optional) Select one or more NSX context profile for the firewall rule. For details on context profiles creation, see Context Profiles in the *NSX Administration Guide*.
Source	a Choose one of the following options. ■ To allow or deny traffic from any source address, toggle on **Any Source**. ■ To allow or deny traffic from specific firewall groups, , click **Firewall Groups** and select the firewall groups from the list. ■ To enter IP addresses, CIDR blocks, or IP ranges manually, click **Firewall IP Addresses**, then click **Add** and enter the individual IP addresses, CIDR blocks, or ranges. b Click **Keep**.
Destination	a Choose one of the following options. ■ To allow or deny traffic to any destination address, toggle on **Any Destination**. ■ To allow or deny traffic to specific firewall groups, click **Firewall Groups** and select the firewall groups from the list. ■ To enter IP addresses, CIDR blocks, or IP ranges manually, click **Firewall IP Addresses**, then click **Add** and enter the individual IP addresses, CIDR blocks, or ranges. b Click **Keep**.
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, without notifying the blocked client select **Drop**. ■ To block traffic from or to the specified sources, destinations, and services, and to notify the blocked client that traffic was rejected, select **Reject**.
IP Protocol	Select whether to apply the rule to IPv4 or IPv6 traffic.
Applied To	(Optional) From the drop-down menu, select a spectific network to which to apply the rule. You can select either an organization VDC network for which distributed routing is deactivated or an external network uplink.

Option	Description
Logging	To have the address translation performed by this rule logged, turn on the **Logging** toggle. After you create the rule, in the Logging ID text box, you can see the unique NSX firewall rule ID that the system generates upon the rule creation.
Comment	(Optional) Add a comment to the firewall rule.

7 Click **Save**.

8 To change the position of the firewall rule, select the rule, click **Move to**, and, from the drop-down menu, select a new position.

9 To configure additional rules, repeat these steps.

Results

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 Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

To change the source IP address from a private to a public IP address, you create a source NAT (SNAT) rule. To change the destination IP address from a public to a private IP address, you create a destination NAT (DNAT) rule.

When you configure a SNAT or a DNAT rule on an edge gateway in the VMware Cloud Director environment, you always configure the rule from the perspective of your organization VDC.

An 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 NO SNAT rule prevents the translation of the internal IP address of packets sent from an organization VDC 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.

A NO DNAT rule prevents the translation of the external IP address of packets received by an organization VDC from an external network or from another organization VDC network.

VMware Cloud Director supports automatic route redistribution when you use NAT services on an NSX edge gateway.

Important If you are using Tanzu Kubernetes clusters, make note of the system SNAT rule created on the edge gateway to avoid creating a conflicting rule.

Prerequisites

Verify that the public IP addresses are added to the edge gateway interface on which you want to add the rule.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the edge gateway and, under **Services**, click **NAT**.
4. To add a rule, click **New**.
5. Configure an SNAT or NO SNAT rule (inside going outside).

Option	Description
Name	Enter a meaningful name for the rule.
Description	(Optional) Enter a description for the rule.
Interface type	From the drop-down menu, select SNAT or NO SNAT.
External IP	Depending on the type of rule that you are creating, choose one of the options. ■ If you are creating a SNAT rule, select or enter the public IP address of the edge gateway for which you are configuring the SNAT rule. ■ If you are creating a NO SNAT rule, leave the text box empty.
Internal IP	Enter the IP address or a list of IP addresses of the virtual machines for which you are configuring SNAT, so that they can send traffic to the external network.

Option	Description
Destination IP	(Optional) If you want the rule to apply only for traffic to a specific domain, enter an IP address for this domain or an IP address list. If you leave this text box blank, the SNAT rule applies to all destinations outside of the local subnet.
Advanced Settings (Optional)	Click the **Advanced Settings** tab for some additional settings. **State** To enable the rule upon creation, toggle on the State option. **Logging** To have the address translation performed by this rule logged, toggle on the **Logging** option. **Priority** If an address has multiple NAT rules, you can assign these rules different priorities to determine the order in which they are applied. A lower value means a higher priority for this rule. **Firewall Match** You can set a firewall match rule to determine how firewall is applied during NAT. From the drop-down menu, select one of the following options. ■ To apply firewall rules to the internal address of a NAT rule, select **Match Internal Address**. ■ To apply firewall rules to the external address of a NAT rule, select **Match External Address**. ■ To skip applying firewall rules, select **Bypass**. **Applied To** Apply this NAT rule only to the selected organization VDC network or to the selected external network selection. You can select either an organization VDC network for which distributed routing is deactivated or an external network uplink.

6 Configure a DNAT or NO DNAT rule (outside going inside).

Option	Description
Name	Enter a meaningful name for the rule.
Description	(Optional) Enter a description for the rule.
Interface type	From the drop-down menu, select DNAT or NO DNAT.
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 IP addresses that are suballocated to the edge gateway.
External Port	(Optional) Enter a port into which the DNAT rule is translating for the packets inbound to the virtual machines.

Option	Description
Internal IP	Depending on the type of rule that you are creating, choose one of the options. ■ If you are creating a DNAT rule, select or enter the IP address or IP addresses list of the virtual machines for which you are configuring DNAT, so that they can receive traffic from the external network. ■ If you are creating a NO DNAT rule, leave the text box empty.
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.
Advanced Settings (Optional)	Click the **Advanced Settings** tab for some additional settings. **State** To enable the rule upon creation, toggle on the State option. **Logging** To have the address translation performed by this rule logged, toggle on the **Logging** option. **Priority** If an address has multiple NAT rules, you can assign these rules different priorities to determine the order in which they are applied. A lower value means a higher priority for this rule. **Firewall Match** You can set a firewall match rule to determine how firewall is applied during NAT. From the drop-down menu, select one of the following options. ■ To apply firewall rules to the internal address of a NAT rule, select **Match Internal Address**. ■ To apply firewall rules to the external address of a NAT rule, select **Match External Address**. ■ To skip applying firewall rules, select **Bypass**. **Applied To** By default, NAT rules are applied to all networks that are connected to the edge gateway. You can select a specific network to which to apply this NAT rule. You can select either an organization VDC network for which distributed routing is deactivated or an external network uplink.

7 Click **Save**.

8 To configure additional rules, repeat these steps.

Configure a DNS Forwarder Service on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the edge gateway and, under **IP Management**, click **DNS**.

4 In the **DNS Forwarder** section, click **Edit**.

5 To enable the DNS Forwarder service, turn on the **State** toggle.

6 Enter a name and, optionally, a description for the default DNS zone.

7 Enter one or more upstream server IP addresses, separated by a comma.

8 Click **Save**.

9 (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**.

Using Non-Distributed Routing with NSX in the VMware Cloud Director Service Provider Admin Portal

VMware Cloud Director supports non-distributed routing for organization VDC networks backed by NSX.

You can configure an NSX edge gateway to allow non-distributed routing and you can connect routed organization VDC networks directly to a tier-1 service router, forcing all VM traffic for a specific network through the service router.

You can use the non-distributed routing feature to create firewall rules and isolate east-west traffic between organization VDC networks that are connected to the same NSX edge gateway.

You can use a non-distributed connection to connect a maximum of 9 organization VDC networks to a single NSX edge gateway.

Configuring DNS after NSX Data Center for vSphere to NSX Migration

If you are migrating your networking infrastructure from NSX Data Center for vSphere to NSX and you were using your organization VDC network gateway address as a DNS server address, you can use non-distributed routing to configure your organization VDC network that is backed by NSX to also use its network gateway's IP address as a DNS server address.

To do that, after you set up your NSX edge gateway and your organization VDC network for non-distributed routing, create a DNAT rule that points to the edge gateway's DNS service and enter the DNS server's IP address in the **Applied to** text box. See Add an SNAT or a DNAT Rule to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Configure an NSX Edge Gateway to Use Non-Distributed Routing in VMware Cloud Director

In VMware Cloud Director, you can configure an existing NSX edge gateway to allow non-distributed routing by editing its general settings.

Prerequisites

- Verify that you are logged in as a **system administrator**.
- Verify that the edge gateway for which you want to enable non-distributed routing is backed by NSX.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway for which you want to enable non-distributed routing.
4. On the left, select the **General** tab, and click **Edit**.
5. To enable non-distributed routing, toggle on the **Allow Non-Distributed Routing** option and click **Save**.

What to do next

Deactivate distributed routing during the creation of an organization VDC network that is connected to this edge gateway. See *Add a Routed Organization Virtual Data Center Network* in the *VMware Cloud Director Tenant Guide*.

Edit the IP Allocations of an NSX Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can allocate multiple IP addresses of an external network to an edge gateway.

Procedure

1. Open Edge Gateway Services.
   a. From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.
   b. In the left panel, click **Edge Gateways**.
   c. Click the radio button next to the name of the target edge gateway, and click **Services**.

2 Click the edge gateway, and click **IP Allocations**.

   In the IP management grids, you can see the IP addresses that are allocated to the edge gateway and the IP addresses that are currently in use by the edge gateway.

3 In the **Allocated IPs** section, click **IP Management**.

   In the **IP Management** grid, you can view the IP usage for each of the external networks that are available for use by the edge gateway.

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

5 Click **Save**.

Results

The IP addresses are allocated to the edge gateway.

What to do next

View the IP addresses that are allocated to the edge gateway, add more IP addresses, or remove them as needed.

Quick IP Allocation in VMware Cloud Director

In VMware Cloud Director, you can allocate IP addresses from an external network subnet to an edge gateway without entering specific IP addresses or IP address ranges by using quick IP allocation.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, and click **Services**.

2 Click the edge gateway and click **IP Allocations**.

   In the IP management grids, you can see the IP addresses that are allocated to the edge gateway and the IP addresses that are currently in use by the edge gateway.

3 In the **Allocated IPs** section, click **Quick IP Allocation**.

4 From the drop-down menu, select a subnet from which to assign IP addresses.

   If multiple subnets are available, selecting **Any** results in the allocation of IP addresses from one or more subnets.

5 Enter the number of IP addresses to allocate to the edge gateway, and click **Save**.

   The number must be less than the number of available IP addresses in the subnet that you selected.

Results

The IP addresses are allocated to the edge gateway.

What to do next

View the IP addresses that are allocated to the edge gateway, add more IP addresses, or remove them as needed.

Create Custom Application Port Profiles in the VMware Cloud Director Service Provider Admin Portal

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, 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 edge gateways in the same organization that are backed by the same NSX-V Manager instance.

Application port profiles in VMware Cloud Director are the inventory equivalent of services in NSX. When you configure a service in NSX, it automatically synchronizes with VMware Cloud Director and it appears in the VMware Cloud Director UI as a custom application port profile.

If you want to configure an NSX service and not sync it with VMware Cloud Director, add the `VCD_IGNORE` tag during the service creation. You can add the `VCD_IGNORE` tag to NSX context profiles that you don't want to sync with VMware Cloud Director. Context profiles are also used for firewall rules, but are not visible in the VMware Cloud Director UI. You can create and view NSX context profiles by using the VMware Cloud Director API. For details on services and context profiles creation, see Add a Service and Context Profiles in *NSX Administration Guide*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the edge gateway.

4 Under **Security**, click **Application Port Profiles**.

5 In the **Custom Applications** section, click **New**.

6 Enter a name and, optionally, a description for the application port profile.

7 Select a protocol from the drop-down menu.

8 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 Edge Gateway Firewall Rule in the VMware Cloud Director Service Provider Admin Portal and Add an SNAT or a DNAT Rule to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Delete Stranded Application Port Profiles from VMware Cloud Director

Stranded application port profiles might prevent you from deleting the organization that contains them. If you need to delete an organization, you can use the VMware Cloud Director API to force delete it and to remove the stranded application port profiles associated with it.

If a **system administrator** deletes an NSX edge gateway without first removing the application port profiles that were created on it, the application port profiles become stranded. Because of this, the organization that contains them cannot be deleted through the VMware Cloud Director UI.

You can use the VMware Cloud Director API to force delete an organization and to delete the stranded application port profiles associated with it from both VMware Cloud Director and NSX.

Procedure

1 Run a DELETE request to delete the organization.

```
DELETE https://api_host/cloudapi/1.0.0/orgs/orgUrn?force=true
```

Use the additional query parameter `force=true` to delete the organization even if it contains objects that are not in an appropriate state.

2 Run a POST request to sync the application port profiles.

```
POST https://api_host/cloudapi/1.0.0/applicationPortProfiles/sync
```

Results

The stranded application port profiles are deleted from both VMware Cloud Director and NSX.

IPsec Policy-Based VPN for NSX Edge Gateways in the VMware Cloud Director Service Provider Admin Portal

Starting with version 10.1, VMware Cloud Director supports site-to-site policy-based IPSec VPN between an NSX edge gateway instance and a remote site.

IPSec VPN offers site-to-site connectivity between an edge gateway and remote sites which also use NSX or which have either third-party hardware routers or VPN gateways that support IPSec.

Policy-based IPSec VPN requires a VPN policy to be applied to packets to determine which traffic is to be protected by IPSec before being passed through a VPN tunnel. This type of VPN is considered static because when a local network topology and configuration change, the VPN policy settings must also be updated to accommodate the changes.

NSX edge gateways support split tunnel configuration, with IPSec traffic taking routing precedence.

VMware Cloud Director supports automatic route redistribution when you use IPSec VPN on an NSX edge gateway.

Configure NSX Policy-Based IPSec VPN in the VMware Cloud Director Service Provider Admin Portal

You can configure site-to-site connectivity between an NSX edge gateway and remote sites. The remote sites must use NSX, have third-party hardware routers, or VPN gateways that support IPSec.

VMware Cloud Director supports automatic route redistribution when you configure IPSec VPN on an NSX edge gateway.

Prerequisites

If you plan to use certificate authentication to secure the IPSec VPN communication, verify that your **system administrator** has uploaded the server certificate for the local NSX edge gateway and a CA certificate for your organization to the VMware Cloud Director certificates library.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Services**, click **IPSec VPN**.

4 To configure an IPSec VPN tunnel, click **New**.

5 Enter a name and, optionally, a description for the IPSec VPN tunnel.

6 To enable the tunnel upon creation, toggle on the **Status** option.

7 (Optional) To enable logging, toggle on the **Logging** option.

8 Select a peer authentication mode.

Option	Description
Pre-Shared Key	Choose a pre-shared key to enter. The pre-shared key must be the same on the other end of the IPSec VPN tunnel.
Certificate	Select site and CA certificates to be used for authentication.

9 From the drop-down menu one of the IP addresses that are available to the edge gateway for the local endpoint.

The IP address must be either the primary IP of the edge gateway, or an IP address that is separately allocated to the edge gateway.

10 Enter at least one local IP subnet address in CIDR notation to use for the IPSec VPN tunnel.

11 Enter the IP address for the remote endpoint.

12 Enter at least one remote IP subnet address in CIDR notation to use for the IPSec VPN tunnel.

13 Enter the remote ID for the peer site.

   The remote ID must match the SAN (Subject Alternative Name) of the remote endpoint certificate, if available. If the remote certificate does not contain a SAN, the remote ID must match the distinguished name of the certificate that is used to secure the remote endpoint, for example, C=US, ST=Massachusetts, O=VMware,OU=VCD, CN=Edge1.

14 Click **Next**.

15 Review your settings and click **Finish**.

16 To verify that the tunnel is functioning, select it and click **View Statisticts**.

   If the tunnel is functioning, **Tunnel Status** and **IKE Service Status** both display `Up`.

Results

The newly created IPSec VPN tunnel is listed in the **IPSec VPN** view. The IPSec VPN tunnel is created with a default security profile.

What to do next

- Configure the remote endpoint of the IPSec VPN tunnel.
- You can edit the IPSec VPN tunnel settings and customize its security profile as needed.

Customize the Security Profile of an IPSec VPN Tunnel in the VMware Cloud Director Service Provider Admin Portal

If you decide not to use the system-generated security profile that was assigned to your IPSec VPN tunnel upon creation, you can customize it.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Services**, click **IPSec VPN**.

4 Select the IPSec VPN tunnel and click **Security Profile Customization**.

5 Configure the IKE profiles.

The Internet Key Exchange (IKE) profiles provide information about the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IKE tunnel.

a Select an IKE protocol version to set up a security association (SA) in the IPSec protocol suite.

Option	Description
IKEv1	When you select this option, IPSec VPN initiates and responds to IKEv1 protocol only.
IKEv2	The default option. When you select this version, IPSec VPN initiates and responds to IKEv2 protocol only.
IKE-Flex	When you select this option, if the tunnel establishment fails with IKEv2 protocol, the source site does not fall back and initiate a connection with the IKEv1 protocol. Instead, if the remote site initiates a connection with the IKEv1 protocol, then the connection is accepted.

b Select a supported encryption algorithm to use during the Internet Key Exchange (IKE) negotiation.

c From the **Digest** drop-down menu, select a secure hashing algorithm to use during the IKE negotiation.

d From the **Diffie-Hellman Group** drop-down menu, select one of the cryptography schemes that allows the peer site and the edge gateway to establish a shared secret over an insecure communications channel.

e (Optional) In the **Association Lifetime** text box, modify the default number of seconds before the IPSec tunnel needs to reestablish.

6 Configure the IPSec VPN tunnel.

a To enable perfect forward secrecy, toggle on the option.

b Select a defragmentation policy.

The defragmentation policy helps to handle defragmentation bits present in the inner packet.

Option	Description
Copy	Copies the defragmentation bit from the inner IP packet to the outer packet.
Clear	Ignores the defragmentation bit present in the inner packet.

c Select a supported encryption algorithm to use during the Internet Key Exchange (IKE) negotiation.

d From the **Digest** drop-down menu, select a secure hashing algorithm to use during the IKE negotiation.

e From the **Diffie-Hellman Group** drop-down menu, select one of the cryptography schemes that allows the peer site and the edge gateway to establish a shared secret over an insecure communications channel.

f (Optional) In the **Association Lifetime** text box, modify the default number of seconds before the IPSec tunnel needs to reestablish.

7 (Optional) In the **Probe Interval** text box, modify the default number of seconds for dead peer detection.

8 Click **Save**.

Results

In the IPSec VPN view, the security profile of the IPSec VPN tunnel displays as **User Defined**.

L2 VPN for NSX Edge Gateways in the VMware Cloud Director Service Provider Admin Portal

VMware Cloud Director supports the creation, deletion and management of L2 VPN tunnels between NSX edge gateways.

With L2 VPN, you can extend your organization VDC by enabling virtual machines to maintain their network connectivity across geographical boundaries while keeping the same IP address. The connection is secured with a route-based IPSec tunnel between the two sides of the tunnel.

You can configure the L2 VPN service on an NSX edge gateway in your VMware Cloud Director environment and create a L2 VPN tunnel. Virtual machines remain on the same subnet, which enables you to extend your organization VDC by stretching its network. This way, 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 an L2 VPN client.

The service type - server or client - that you configure on the first L2 VPN tunnel on an edge gateway determines the session mode for all other L2 VPN tunnels on the edge gateway. You can only configure one client session per edge gateway.

After you create a tunnel, you cannot change its session mode from server to client, or vice versa. For example, if you want to change the session mode on an NSX edge gateway from server to client, you must delete all existing server tunnels from it.

When you create an L2 VPN server tunnel endpoint, a tunnel ID is automatically assigned to the organization VDC network that you stretch, and a peer code is generated. On the client side of the tunnel, you need to add a corresponding network with the same tunnel ID, peer code, and the same subnet.

For more information on L2 VPN for NSX, see *NSX Administration Guide*.

Configure an NSX Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal

The L2 VPN server is the destination NSX edge to which the L2 VPN client is going to connect.

In Server session mode, the NSX edge gateway acts as the server side of the L2 VPN tunnel. It generates peer codes to distribute for client sessions.

You can connect multiple peer sites to a single L2 VPN server.

Prerequisites

- Verify that the NSX edge gateway is connected to a routed organization virtual data center network.
- Verify that your role includes the **Organization vDC Gateway: Configure L2 VPN** right.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.
3. Under **Services**, click **L2 VPN**.
4. To configure an L2 VPN tunnel, click **New**.
5. If this is the first L2 VPN tunnel for this edge gateway, select **Server** session mode and click **Next**.
6. Enter a name and, optionally, a description for the L2 VPN tunnel.
7. Choose a pre-shared key to enter.

   If you change the pre-shared key after the initial configuration of the L2 VPN server, you must reconfigure all client tunnels that use the pre-shared key with a new peer code .
8. To enable the tunnel upon creation, toggle on the **State** option.
9. (Optional) To enable logging, toggle on the **Logging** option.
10. Click **Next**.
11. From the drop-down menu, select one of the IP addresses that are available to the edge gateway for the local endpoint.

    The IP address must be either the primary IP of the edge gateway, or an IP address that is separately allocated to the edge gateway.
12. Enter a subnet address in CIDR notation for the tunnel interface that secures the connection.
13. Enter the IP address for the remote endpoint.
14. Select an initiation mode and click **Next**.

Option	Description
Initiator	The local endpoint initiates the L2 VPN tunnel setup and responds to incoming tunnel setup requests from peer gateways.
Respond Only	The local endpoint only responds to incoming tunnel setup requests, it doesn't initiate the L2 VPN tunnel setup.

15 Select one or more organization VDC networks to which to attach the tunnel and click **Next**.

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

Results

The new L2 VPN tunnel appears in the list.

What to do next

In the **Org VDC Networks** row of the list of L2 VPN tunnels, click **Info** and note the tunnel IDs for the organization VDC networks that you want to stretch.

Copy the L2 VPN Peer Code From An L2 VPN Server Endpoint in the VMware Cloud Director Service Provider Admin Portal

To configure an NSX edge gateway as an L2 VPN client, you must copy the peer code that is generated from the L2 VPN server side of the tunnel.

Prerequisites

Verify that you configured the L2 VPN server endpoint of the tunnel.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Services**, click **L2 VPN**.

4 Select the L2 VPN tunnel for which you want to copy the peer code.

5 Click the **Copy peer code** button.

Results

The peer code is copied to the clipboard.

Configure an NSX Edge Gateway as an L2 VPN Client in the VMware Cloud Director Service Provider Admin Portal

You can create only one client tunnel on an NSX edge gateway.

Prerequisites

- Verify that your role includes the **Organization vDC Gateway: Configure L2 VPN** right.
- Verify that there are no other client L2 VPN tunnels configured on this edge gateway.
- Configure an NSX Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal.
- Copy the peer code of the L2 VPN server endpoint. See Copy the L2 VPN Peer Code From An L2 VPN Server Endpoint in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Services**, click **L2 VPN**.

4 To configure an L2 VPN tunnel, click **New**.

5 If this is the first L2 VPN tunnel for this edge gateway, select **Client** session mode and click **Next**.

6 Enter a name and, optionally, a description for the L2 VPN tunnel.

7 Paste the peer code from the L2 VPN Server tunnel that you wish to connect to.

8 To enable the tunnel upon creation, toggle on the **State** option.

9 (Optional) To enable logging, toggle on the **Logging** option.

10 Click **Next**.

11 Enter one of the IP addresses that are available to the edge gateway for the local endpoint.

The IP address must be the one that you entered as a remote endpoint on the server side of the tunnel.

12 Enter the IP address for the remote endpoint.

The IP address must be the one that you entered as a local endpoint on the server side of the tunnel.

13 Select the organization VDC network or networks to which to attach the tunnel, specify the tunnel ID for each network, and click **Next**.

The tunnel IDs that you use for each organization VDC network must be the same as the tunnel IDs for the organization VDC networks on the server side.

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

Configure Static Routing on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

If you want to use a network traffic route that is not publicly advertised within your environment, you can manually configure a static route on an NSX edge gateway.

View the Static Routes on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can view the both the read-only and the editable static routes on an NSX edge gateway.

You can view both the editable and the read-only static routes on an edge gateway. A read-only static route is configured in NSX Manager and can have more than 5 next hops. However, in VMware Cloud Director, you can view only the first 5 hops of a read-only static route.

Prerequisites

Verify that your role includes the **Gateway Service: Static Routing View Only** right.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, and click **Services**.

2 Click the edge gateway and, under Routing, click **Static Routes**.

3 View the static routes on the edge gateway.

Configure a Static Route on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can manually configure a static route on an NSX edge gateway.

Prerequisites

Verify that your role includes the **Gateway Service: Static Routing Configure** right.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, and click **Services**.

2 Click the edge gateway and, under Routing, click **Static Routes**.

3 Click **New**.

4 Enter a name and, optionally, a description for the new route.

5 Enter a network address in CIDR format to which to direct network traffic.

6 Click the **Next Hops** tab and click **Add**.

7 Add a next hop IP address.

8 Specify an admin distance.

   The admin distance is used to choose which route to use when there are multiple routes for a specific network. The lower the admin distance, the higher the preference for the route. Static routes have a default administrative distance of 1.

9 (Optional) From the drop-down list, select a scope for the static route.

   The scope is either an organization VDC network or an external network connection in which the next hop is located.

10 Click **Save**.

11 To add additional next hops, repeat steps 7 through 11.

You can add up to 5 next hops.

Configure Dedicated Provider Gateway Services in the VMware Cloud Director Service Provider Admin Portal

When you use a dedicated provider gateway, you can configure additional routing services, such as route advertisement and border gateway protocol (BGP) configuration.

If you are using a provider gateway with legacy IP blocks, to provide a fully routed network topology in a virtual data center, you can dedicate a provider gateway to a specific NSX edge gateway.

If you are using a provider gateway with IP spaces, you can configure static routes and BGP on the provider gateway itself, and you can manage route advertisement on the organization VDC network level.

Dedicated Provider Gateways in VMware Cloud Director

If you are using a provider gateway with legacy IP blocks, to provide a fully routed network topology in a VMware Cloud Director virtual data center, you can dedicate the provider gateway to a specific NSX edge gateway.

If you want to use provider gateways with IP spaces, see Managing Provider Gateways in Your VMware Cloud Director.

In this dedicated provider gateway configuration, there is a one-to-one relationship between the provider gateway and the VMware Cloud Director edge gateway, and no other VMware Cloud Director edge gateways can connect to the provider gateway.

An edge gateway or a VRF-lite gateway that is associated with a dedicated provider gateway is part of the tenant networking stack. The provider gateway is considered a part of the VMware Cloud Director network routing domain.

Dedicating a provider gateway to an VMware Cloud Director edge gateway provides tenants with additional edge gateway services, such as route advertisement management and border gateway protocol (BGP) configuration.

The tenant can decide which of the tenant networks that are attached to the edge gateway to advertise to the provider gateway. This makes possible a mixture of NAT-routed and fully routed organization virtual data center networks.

You can dedicate a provider gateway to an VMware Cloud Director edge gateway either during the edge gateway creation or later, by editing the edge gateway general settings.

Manage Route Advertisement in the VMware Cloud Director Service Provider Admin Portal

By using route advertisement, you can create a fully routed network environment in an organization virtual data center (VDC).

Note If you are using IP spaces, route advertisement is managed at the organization VDC network level. When you create an IP space, configuring its network topology includes allowing route advertisement for the routed networks associated with the IP space from the edge gateway to the provider gateway. See Enable Route Advertisement For an IP Space in VMware Cloud Director and Create a Routed Organization VDC Network.

You can decide which of the network subnets that are attached to the edge gateway backed by NSX to advertise to the dedicated provider gateway.

If a subnet is not added to the advertisement filter, the route to it is not advertised to the provider gateway and the subnet remains private.

Note VMware Cloud Director advertises any organization VDC network that falls within the advertised route. Because of that, you do not need to create a filter for each subnet that is part of an advertised network.

Route advertisement is automatically configured on the NSX edge gateway.

VMware Cloud Director supports automatic route redistribution when you use route advertisement on an NSX edge gateway. Route redistribution is automatically configured on the tier-0 logical router which represents the dedicated provider gateway.

Prerequisites

- Verify that you have dedicated a provider gateway that used IP blocks to a VMware Cloud Director edge gateway backed by NSX in the organization. See Dedicated Provider Gateways in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Routing**, click **Route Advertisement** and **Edit**.

4 To add a subnet to be advertised, click **Add**.

5 Add an IPv4 or IPv6 subnet.

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

Configure BGP General Settings on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can configure an external or internal Border Gateway Protocol (eBGP or iBGP) connection between a VMware Cloud Director edge gateway backed by NSX that has a dedicated provider gateway and a router in your physical infrastructure.

Note Starting with VMware Cloud Director 10.5, if you are using IP spaces, you configure BGP settings on your provider gateway. See Configure BGP on a Provider Gateway That Uses IP Spaces in the VMware Cloud Director Service Provider Admin Portal.

BGP makes core routing decisions by using a table of IP networks, or prefixes, which designate multiple routes between autonomous systems (AS).

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.

Note In an edge gateway that is connected to an external network backed by a VRF gateway, graceful restart settings are read-only. You can edit these settings on the parent tier-0 in NSX.

If you are using NSX 4.1, you can edit the the local AS number on an edge gateway that is backed by a VRF gateway. In earlier versions, the local AS number setting is read-only and can be configured by a **system administrator** on the parent tier-0 in NSX.

Prerequisites

- Verify that you dedicated a provider gateway that uses IP blocks to a VMware Cloud Director edge gateway backed by NSX in the organization. See Dedicated Provider Gateways in VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.
3. Under **Routing**, click **BGP** and, under **Configuration**, click **Edit**.
4. Toggle on the **Status** option to enable BGP.
5. Enter an autonomous system (AS) ID number to use for the local AS feature of the protocol.

   VMware Cloud Director assigns the local AS number to the edge gateway. The edge gateway advertises this ID when it connects with its BGP neighbors in other autonomous systems.

6 From the drop-down menu, select a **Graceful Restart Mode** option.

Option	Description
Helper and graceful restart	It is not a best practice to enable the graceful restart capability on the edge gateway because the BGP peerings from all gateways are always active. In case of a failover, the graceful restart capability increases the time a remote neighbor takes to select an alternate tier-0 gateway. This delays BFD-based convergence. **Note** The edge gateway configuration applies to all BGP neighbors unless the neighbor-specific configuration overrides it.
Helper only	Useful for reducing or eliminating the disruption of traffic associated with routes learned from a neighbor that is capable of graceful restart. The neighbor must be able to preserve its forwarding table while it undergoes a restart.
Disable	Deactivate graceful restart mode on the edge gateway.

7 (Optional) Change the default value for the graceful restart timer.

8 (Optional) Change the default value for the stale route timer.

9 Toggle on the **ECMP** option to enable ECMP.

10 Click **Save**.

What to do next

- Create an IP Prefix List in the VMware Cloud Director Service Provider Admin Portal
- Add a BGP Neighbor in the VMware Cloud Director Service Provider Admin Portal

Create an IP Prefix List in the VMware Cloud Director Service Provider Admin Portal

You can create IP prefix lists which contain single or multiple IP addresses. You use IP prefix lists to assign BGP neighbors with access permissions for route advertisement.

The IP prefix lists are referenced through BGP neighbor filters to limit the number of BGP updates that are exchanged between BGP peers. By using route filtering, you can reduce the amount of system resources needed for BGP updates.

For example, you can add the IP address 192.168.100.3/27 to the IP prefix list and deny the route from being redistributed to the edge gateway.

You can also append an IP address with `less than or equal to` (le) and `greater than or equal to` (ge) modifiers to grant or limit route redistribution. For example, 192.168.100.3/27 ge 26 le 32 modifiers match subnet masks greater than or equal to 26-bits and less than or equal to 32-bits in length.

Prerequisites

- Verify that you have dedicated a provider gateway that used IP blocks to a VMware Cloud Director edge gateway backed by NSX in the organization. See Dedicated Provider Gateways in VMware Cloud Director.
- Configure BGP General Settings on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.
3. Under **Routing**, click **BGP** and **IP Prefix Lists**.
4. To add an IP prefix list, click **New**.
5. Enter a name and, optionally, a description for the prefix list.
6. Click **New** and add a CIDR notation for the prefix.
7. From the drop-down menu, select an action to apply to the prefix.
8. (Optional) Enter `greater than or equal to` and `less than or equal to` modifiers to grant or limit route redistribution.

What to do next

- You can edit or delete the IP prefix list as needed.
- Configure route filtering. See Add a BGP Neighbor in the VMware Cloud Director Service Provider Admin Portal.

Add a BGP Neighbor in the VMware Cloud Director Service Provider Admin Portal

You can configure individual settings for the BGP routing neighbors when you add them.

Prerequisites

- Verify that you have dedicated a provider gateway that used IP blocks to a VMware Cloud Director edge gateway backed by NSX in the organization. See Dedicated Provider Gateways in VMware Cloud Director.
- Verify that you configured the global BGP settings for the edge gateway. See Configure BGP General Settings on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- If you use route filtering, verify that you created IP prefix lists. See Create an IP Prefix List in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Under **Routing**, click **BGP** and **Neighbors**.

4 To add a new BGP neighbor, click **New**.

5 Enter the general settings for the new BGP neighbor.

   a Enter an IPv4 or IPv6 address for the new BGP neighbor.

   b Enter a remote Autonomous System (AS) number in ASPLAIN format.

   c Enter a time interval between sending keep-alive messages to a BGP peer.

   d Enter a time interval before declaring a BGP peer dead.

   e From the drop-down menu, select a **Graceful Restart Mode** option for this neighbor.

Option	Description
Disable	Overrides the global edge gateway settings and deactivates graceful restart mode for this neighbor.
Helper only	Overrides the global edge gateway settings and configures graceful restart mode as **Helper only** for this neighbor.
Graceful restart and Helper	Overrides the global edge gateway settings and configures graceful restart mode as **Graceful restart and Helper** for this neighbor.

   f Toggle on the **AllowAS-in** toggle to enable receiving routes with the same AS.

   g If the BGP neighbor requires authentication, enter the password for the BGP neighbor.

6 Configure the Bidirectional Forwarding Detection (BFD) settings for the new BGP neighbor.

   a (Optional) Toggle on the **BFD** option to enable BFD for failure detection.

   b In the BDF interval text box, define the time interval for sending heartbeat packets.

   c In the **Dead Multiple** text box, enter the number of times the BGP neighbor can fail to send heartbeat packets before the BFD declares it is down.

7 (Optional) Configure route filtering.

   a From the **IP Address Family** drop-down menu, select an IP address family.

   b To configure an inbound filter, select an IP prefix list.

   c To configure an outbound filter, select an IP prefix list.

8 Click **Save**.

What to do next

You can view the status of each BGP neighbor, edit, or delete BGP neighbors as needed.

Managing NSX Advanced Load Balancing on an NSX Edge Gateway in VMware Cloud Director

As a **system administrator**, in VMware Cloud Director, you enable load balancing on an NSX gateway and assign a service engine group to the edge gateway.

An **organization administrator** creates load balancer server pools and virtual services.

Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

Before an **organization administrator** can configure load balancing services, a **system administrator** must enable the load balancer on the NSX edge gateway.

You can add an IPv6 service network either during the enablement of NSX Advanced Load Balancer or later.

Starting with version 10.4.1, VMware Cloud Director supports transparent load balancing. Transparent mode indicates whether the source IP address of the client in incoming packets is visible to the backend servers.

Prerequisites

- Verify that you are logged in as a **system administrator**.
- Verify that you integrated VMware NSX Advanced Load Balancer in your cloud infrastructure. For more information on managing NSX Advanced Load Balancer, see *VMware Cloud Director Service Provider Admin Guide*.
- If you want to use an IPv6 service network to configure IPv6 virtual IP addresses for virtual services and IPv6 load balancer pool members, verify that you configured DHCPv6 mode with SLAAC enabled on the NSX edge gateway.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway on which you want to enable load balancing.
4. Under Load Balancer, click **General Settings**.
5. Click **Edit** and toggle on the **Load Balancer State** option.
6. To activate client IP preservation, toggle on the **Tranparent Mode** option.

7 If prompted, select a feature set from the drop-down menu.

If you enabled the edge gateway with a **Premium** feature set, you can only configure the edge gateway to use **Premium** features. If you enabled the gateway with a **Standard** feature set, you can choose to use either **Standard** or **Premium** features.

Option	Description
Standard	The standard feature set provides the load balancing features included in VMware NSX Advanced Load Balancer Basic Edition.
Premium	The premium feature set provides access to some **Premium** features, such as, for example, additional load balancing pool algorithm types and pool persistence profiles, virtual service analytics, pool analytics, multiple virtual service ports, and additional virtual service application profile types.

8 Enter CIDR for service network subnets from which to use IP addresses for creation of virtual services.

You can use IPv4 networks, IPv6 networks, or both.

You can use the default IPv4 service network subnet by selecting the **Use Default** check box.

9 Click **Save**.

What to do next

Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

Before an **organization administrator** can configure load balancing services on an NSX edge gateway, a **system administrator** must assign a service engine group to the edge gateway.

The load balancing compute infrastructure provided by NSX Advanced Load Balancer is organized into service engine groups. A **system administrator** can assign one or more service engine groups to an NSX edge gateway.

All service engine groups that are assigned to a single edge gateway use the same service network.

If you enabled the edge gateway with a **Premium** feature set, you can only configure service engine groups with **Premium** features. If you enabled the gateway with a **Standard** feature set, you can choose to use either **Standard** or **Premium** features for a service engine group and you can assign service engine groups with different feature sets to a single load balancer.

Prerequisites

- Verify that you are logged in as a **system administrator**.
- Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway to which you want to assign a service engine group.

4 Under Load Balancer, click **Service Engine Groups**.

5 Click **Add**.

6 Select an available service engine group from the list.

7 Enter a number for the maximum number of virtual services that can be placed on the edge gateway.

8 Enter a number for the guaranteed virtual services available to the edge gateway.

9 To confirm your settings, click **Save**.

Edit the Settings of a Service Engine Group in the VMware Cloud Director Service Provider Admin Portal

You can edit the maximum number of supported virtual services and the number of reserved virtual services for a service engine group.

After you sync a service engine group, if the new maximum number of supported virtual services is lower than the number of reserved virtual services, the service engine group is marked as overallocated.

If a service engine group is overallocated, the creation of a new virtual service might fail, even if the edge gateway on which you create the virtual service has enough reserved capacity.

To avoid failure of virtual service creation, when you edit the settings of a service engine group, do not reduce the maximum number of supported virtual services below the number of initially reserved virtual services.

Prerequisites

- Verify that you are logged in as a **system administrator**.
- Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Verify that the service engine group that you want to edit has a shared reservation model.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway to which the service engine group is assigned.

4 Under Load Balancer, click **Service Engine Groups**.

5 Click **Edit**.

6 Edit the number for the maximum allowed virtual services that the edge gateway can use.

   Do not reduce the number unless mandatory. Otherwise, you might face failures when you create virtual services.

7 Edit the number for the guaranteed virtual services available to the edge gateway.

8 Click **Save**.

Add a Load Balancer Server Pool in the VMware Cloud Director Service Provider Admin Portal

A server pool is a group of one or more servers that you configure to run the same application and to provide high availability.

Prerequisites

- Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway for which you want to configure a load balancer pool.

4 Under Load Balancer, click **Pools**, and then click **Add**.

5 Configure the general settings for the load balancer pool.

a Enter a meaningful name and, optionally, a description for the server pool.

b Select an algorithm balancing method.

The load balancing algorithm defines how incoming connections are distributed among the members of the server pool.

The algorithm methods available to you differ depending on the feature set that you enabled on the edge gateway - Standard or Premium.

Option	Description
Least Connections	Use this method to send new connections to the server that currently has the fewest connections.
Weighted Least Connections	Send new connections to pool members based on the weight assigned to each pool member.
Round Robin	Send new connections to the next eligible server in the pool in a sequential order.
Weighted Round Robin	Send connections to pool members based on the weight assigned to each pool member.
Fastest Response	Available in Premium. New connections are sent to the server that provides the fastest response to new connections or requests.
Consistent Hash	New connections are distributed across the servers by using the IP address of the client to generate an IP hash key.
Least Load	Available in Premium. New connections are sent to the server with the lightest load, regardless of the number of connections that server has.
Fewest Servers	Available in Premium. Instead of attempting to distribute all connections or requests across all servers, the load balancer determines the fewest number of servers required to satisfy the current client load.
Random	Available in Premium. The load balancer picks servers at random.
Fewest Tasks	Available in Premium. Load is adaptively balanced, based on the server feedback.
Core Affinity	Available in Premium. Each CPU core uses a subset of servers, and each server is used by a subset of cores. Essentially, it provides a many-to-many mapping between servers and cores.

c To enable the server pool upon creation, toggle on the **State** option.

d Enter a default destination server port to be used for the traffic to the pool member.

e (Optional) In the **Graceful Disable Timeout** text box, enter the maximum time in minutes to gracefully deactivate a pool member.

The virtual service waits for the specified time before closing the existing connections to deactivated members.

f (Optional) To enable a passive health monitor, toggle on the **Passive Health Monitor** option.

g (Optional) Select an active health monitor.

Option	Description
HTTP	An HTTP request and response are used to validate the health.
HTTPS	Used against HTTPS encrypted web servers to validate the health.
TCP	A TCP connection is used to validate the health.
UDP	A UDP datagram is used to validate the health.
PING	An ICMP ping is used to validate the health.

6 Add a member to the server pool.

a Click the **Members** tab and click **Add**.

b To add an IP address for a pool member, select **IP Address** and enter an IP address.

c To add a group pool member, select **Groups** and select a group from the list.

d Toggle on the **State** option to enable the pool member.

e (Optional) Add a custom port for the server pool member.

The port number defaults to the destination port that you entered for the pool.

f Enter a ratio for the pool member.

The ratio of each pool member denotes the traffic that goes to each server pool member. A server with a ratio of 2 gets twice as much traffic as a server with a ratio of 1. The default value is 1.

7 On the **SSL Settings** tab, configure the SSL settings for validating the certificates presented by the members of the load balancer pool.

a To enable SSL, toggle on the **SSL Enable** option.

b To hide certificates with private keys and see a list of CA certificates only, select the **Hide service certificates** check box.

8 To enable common name check for server certificates, toggle on the **Common Name Check** option and enter up to 10 domain names for the pool.

9 Click **Save**.

What to do next

Create a Virtual Service in the VMware Cloud Director Service Provider Admin Portal.

Create a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

A virtual service listens for traffic to an IP address, processes client requests, and directs valid requests to a member of the load balancer server pool.

A virtual service is a combination of an IP address and a port that uses a single network protocol. The virtual service is advertised to outside networks and is listening for client requests. When a client connects to the virtual service, the load balancer directs the request to a member of the load balancer server pool that you configured.

To secure SSL termination for a virtual service, you can use a certificate from the certificate library. For more information, see Import Certificates to the Certificates Library Using Your VMware Cloud Director Service Provider Admin Portal.

Starting with VMware Cloud Director 10.4, when you create a virtual service, you can provide it either with an IPv4 address, or with an IPv6 address, or with both.

Virtual services can share the same virtual IP address if you configure them to use different ports.

Prerequisites

- Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Add a Load Balancer Server Pool in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway on which you want to create a virtual service.
4. Under Load Balancer, click **Virtual Services**, and then click **Add**.
5. Enter a meaningful name and, optionally, a description, for the virtual service.
6. To activate the virtual service upon creation, toggle on the **Enabled** option.
7. To activate client IP address preservation, toggle on the **Preserve Client IP** option.
8. Select a service engine group for the virtual service.
9. Select a load balancer pool for the virtual service.

   If you activated client IP address preservation, you can only select a group pool member.
10. Enter a virtual IP address for the virtual service.

    If you didn't activate client IP address preservation, you can add either an IPv4 address, an IPv6 address, or both.

    If you activated client IP address preservation, you can enter only an IPv4 address.

11 Select the virtual service type.

Option	Description
HTTP	The virtual service listens for non-secure layer 7 HTTP requests. When you select this service type, it autopopulates the service port text box to 80, which you can replace with another valid port number.
HTTPS	The virtual service listens for secure layer 7 HTTPS requests. When you select this service type, it autopopulates the service port text box to port 443, which you can replace with another valid port number. Select an SSL certificate to be used for SSL termination.
L4	The virtual service listens for layer 4 requests. When you select this service type, it autopopulates the service port text box to 80, which you can replace with another valid port number.
L4 TLS	The virtual service listens for secure layer 4 TLS requests. When you select this service type, it autopopulates the service port text box to TCP port 443, which you can replace with another valid port number. Select an SSL certificate to be used for SSL termination.

12 Click **Save**.

Configuring HTTP Policies for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

Starting with version 10.5, VMware Cloud Director supports configuration of virtual service policies that you can use to customize HTTP security, HTTP requests, and HTTP responses.

You can use virtual service HTTP policies to control security, client request attributes, and application response attributes.

A virtual service policy consists of match criteria and actions that function similarly to an `if-then` statement. If match criteria are met, VMware Cloud Director performs the corresponding action.

Each policy that you configure for a virtual service includes one or more rules that are evaluated in the order that you specify. If a rule is successfully evaluated and applied, no further rules in the policy are evaluated.

You can apply HTTP rules only to a layer-7 virtual service.

HTTP Request Rules

You can use HTTP request rules to modify requests before they are either forwarded to the application, used as a basis for content switching, or discarded.

HTTP Response Rules

You can use HTTP response rules to evaluate and modify the response and response attributes that the application returns.

HTTP Security Rules

You can use HTTP security rules to configure allowing or denying certain requests, to close the TCP connection, to redirect a request to HTTPS, or to apply a rate limit.

After configuring the HTTP custom policies for a virtual service, you can reorder, update, and delete them, as needed.

Configure HTTP Request Policies for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

You can use request policies to modify HTTP requests before they are forwarded to the application.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway, and under Load Balancer, click **Virtual Services**.
4. Click the vertical ellipsis (⋮) on the left of the virtual service name and select **Configure Policies**.
5. Click **HTTP Request**, and click **New**.
6. Enter a name for the rule.
7. To activate the rule upon creation, toggle on the **State** option.
8. Under Match Criteria, click **New**.
9. Select one or more match criteria and enter the necessary input.

Option	Description
Client IP Address	a Select whether to perform an action if the client IP matches or doesn't match the value that you enter. b Enter an IPv4 address, or an IPv6 address, or a range, or a CIDR notation. c (Optional) To add more IP addresses, click **Add IP**.
Service Port	a Select whether to perform an action if the virtual service port matches or doesn't match the value that you enter. b Enter a port or a list of ports in a comma-separated list.
Protocol Type	Select a type of protocol.
HTTP Method	a Select whether to perform an action if the HTTP method matches or doesn't match the value that you enter. b Select one or more HTTP methods used by the client request.
Path	a Select a criteria for the path. b Enter a path string. **Note** The path doesn't need to begin with a forward slash (/). c (Optional) To add more paths, click **Add Path**.

Option	Description
Query	a Enter text that is part of a query string. b (Optional) To enter more queries, click **Add Query**.
Request Headers	a Select a criteria for the request header. b Enter a name for the header. c Enter one or more values for the header. d To add more headers, click **Add Header**.
Cookie	a Select a criteria for the cookie. b Enter a name for the cookie. c Enter a value.

10 Select an action to perform upon a match.

Option	Description
Redirect	To redirect the request, enter the necessary information. a Select a redirect protocol. b Enter a port. c Select a status code. d Enter a custom host name. e Enter a path. f To keep the original query parameters in the modified request, select the **Keep Query** check box.
Modify Header	To modify the request header, follow the steps. a Select whether to remove, add, or replace the HTTP header. b Enter the custom header value. c To configure additional header modification actions, click **Add Action** and repeat substeps a. and b..
Rewrite URL	a Enter a custom host header. b Enter an existing custom path. c To keep the original query parameters in the modified request, select the **Keep Query** check box. d (Optional) If you selected **Keep Query**, add more query parameters.

11 Click **Add**.

12 To add another rule, repeat steps 6 through 12.

13 To move a rule up or down the list, click the vertical ellipsis (⋮) on the left of the rule name and select the desired action.

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

Configure HTTP Response Policies for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

You can use HTTP response policies to evaluate and modify application responses.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway, and under Load Balancer, click **Virtual Services**.

4 Click the vertical ellipsis (⋮) on the left of the virtual service name and select **Configure Policies**.

5 Select **HTTP Response** and click **New**.

6 Enter a name for the rule.

7 To activate the rule upon creation, toggle on the **State** option.

8 Under Match Criteria, click **New**.

9 Select one or more match criteria and enter the necessary input.

Match Criteria	Input
Client IP Address	a Select whether to perform an action if the client IP matches or doesn't match the value that you enter. b Enter an IPv4 address, or an IPv6 address, or a range, or a CIDR notation. c (Optional) To add additional IP addresses, click **Add IP**.
Service Port	a Select whether to perform an action if the virtual service port matches or doesn't match the value that you enter. b Enter a port or a list of ports in a comma-separated list.
Protocol Type	Select a type of protocol.
HTTP Method	a Select whether to perform an action if the HTTP method matches or doesn't match the value that you enter. b Select one or more HTTP methods used by the client request.
Path	a Select a criteria for the path. b Enter a path string. **Note** The path doesn't need to begin with a forward slash (/). c (Optional) To add additional paths, click **Add Path**.
Query	a Enter text that is part of a query string. b (Optional) To enter additional queries, click **Add Query**.
Request Headers	a Select a criteria for the request header. b Enter a name for the header. c Enter one or more values for the header. d To add additional headers, click **Add Header**.
Cookie	a Select a criteria for the cookie. b Enter a name for the cookie. c Enter a value.

10. Select an action to perform upon a match.

Option	Description
Rewrite Location Header	a Select a protocol. b Enter a port to include in the header. c Enter a custom host name. d Enter a path. e To keep the original query parameters in the response, select the **Keep Query** check box.
Modify Header	a Select whether to remove, add, or replace the HTTP header. b Enter the custom header value. c To configure additional header modification actions, click **Add Action** and repeat substeps a. and b..

11. Click **Add**.
12. To add another rule, repeat steps 6 through 12.
13. To move a rule up or down the list, click the vertical ellipsis (⋮) on the left of the rule name and select the desired action.
14. To save your changes, click **Save**.

Configure HTTP Security Policies for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

You can use HTTP security policies to define actions such as allowing or denying a connection, redirecting to HTTPS, or responding with a static page.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the NSX edge gateway, and under Load Balancer, click **Virtual Services**.
4. Click the vertical ellipsis (⋮) on the left of the virtual service name and select **Configure Policies**.
5. Click **HTTP Security**, and click **New**.
6. Enter a name for the rule.
7. To activate the rule upon creation, toggle on the **State** option.
8. Under Match Criteria, click **New**.

9 Select one or more match criteria and enter the necessary input.

Match Criteria	Input
Client IP Address	a Select whether to perform an action if the client IP matches or doesn't match the value that you enter. b Enter an IPv4 address, or an IPv6 address, or a range, or a CIDR notation. c (Optional) To add additional IP addresses, click **Add IP**.
Service Port	a Select whether to perform an action if the virtual service port matches or doesn't match the value that you enter. b Enter a port or a list of ports in a comma-separated list.
Protocol Type	Select a type of protocol.
HTTP Method	a Select whether to perform an action if the HTTP method matches or doesn't match the value that you enter. b Select one or more HTTP methods used by the client request.
Path	a Select a criteria for the path. b Enter a path string. **Note** The path doesn't need to begin with a forward slash (/). c (Optional) To add additional paths, click **Add Path**.
Query	a Enter text that is part of a query string. b (Optional) To enter additional queries, click **Add Query**.
Request Headers	a Select a criteria for the request header. b Enter a name for the header. c Enter one or more values for the header. d To add additional headers, click **Add Header**.
Cookie	a Select a criteria for the cookie. b Enter a name for the cookie. c Enter a value.

10 Select an action to perform upon a match.

Action	Input
Connection	Select whether to allow or to close the connection.
Rate Limit	a Enter a maximum number of connections, requests or packets to allow for a period of time. b Enter a value for the time period in seconds. c Select an action to perform when the maximum count of requests within the specified period of time is reached.
Redirects to HTTPS	Enter an HTTPS port to redirect HTTP requests.
Send Response	Select a status code and, optionally, upload a file to render in response.

11 Click **Add**.

12 To add another rule, repeat steps 6 through 12.

13 To move a rule up or down the list, click the vertical ellipsis (⋮) on the left of the rule name and select the desired action.

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

View the Logs for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can view detailed logs for the virtual services that you configured.

The virtual service logs include WAF signature violation logs that are always categorized as critical.

Prerequisites

- Enable Load Balancer on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Assign a Service Engine Group to an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Add a Load Balancer Server Pool in the VMware Cloud Director Service Provider Admin Portal.
- Create a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway on which the virtual service is configured.

4 Click the virtual service name and then click the **Logs** tab.

A list of the virtual service logs for the selected period is displayed. You can filter the results by log type (if non-critical logging is enabled), client IP, URI, request type and response.

5 If you suspect that the WAF signature violations list contains a false positive, you can check the WAF recommendations.

The recommendations feature provides suggestions for WAF settings remediation to avoid similar false positive reports in the future.

a On the right hand side of the Log Details, click **Recommendations**.

b Review the proposed changes, the reasoning for them and the associated risks.

Note that accepting the recommendations results in a reconfiguration of the WAF settings that might be difficult to undo.

c If you choose to implement the proposed remediation changes, click **Accept**.

6 To change the time interval for which you are seeing virtual service logs, select a new interval from the drop-down menu or select **Custom** and specify a time period.

7 To view the details for a specific log event, click the expand button on the left of the log name.

   Information about the logged event is displayed, including WAF signature violations, if any, and details about the client request, any actions, and the application response.

8 If necessary, export the logs for the virtual service in CSV format.

   a On the right side of the screen, click **Export Logs**.

   b (Optional) Select the **Friendly Field Names** check box if you want to use friendly column headers.

      If you you deselect the check box, the output document will use the field names from the original logs in the column headers.

   c (Optional) Select the **Sanitize Data** check box if you want the log data to be sanitized by prepending tab characters to data that otherwise could be interpreted as a spreadsheet formula.

      Deselect the check box if you do not want the data to be sanitized, for example, if the added tabs may prevent a script from reading it correctly.

   d (Optional) If you want to export only specific columns, deselect the **Export All Columns** check box and select the names of the columns that you want to export.

   e Click **Export**.

Configure WAF for a Virtual Service in the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, you can use the web application firewall feature of NSX Advanced Load Balancer within your VMware Cloud Director environment to protect your virtual services from attacks and to proactively prevent threats.

When you enable WAF for a virtual service in VMware Cloud Director, this creates a WAF policy, a WAF profile, and WAF signatures to attach to the virtual service.

Prerequisites

- Familiarize yourself with the NSX Advanced Load Balancer WAF Guide. See VMware NSX Advanced Load Balancer Documentation.
- Verify that you assigned a service engine group with a Premium feature set to the NSX edge gateway.
- Verify that you are logged in as an **organization administrator**.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway on which the virtual service is configured.

4 Click the virtual service and click **WAF**.

5 Under General, click **Edit**.

6 Toggle on the **WAF State** option.

7 Select a WAF mode.

Option	Description
Detection	The WAF policy evaluates and processes the incoming request, but does not perform a blocking action. A log entry is created when the request is flagged.
Enforcement	The WAF policy evaluates the request and blocks the request based on the specified rules. The corresponding log entry is marked as `REJECTED`.

8 Click **Save**.

What to do next

If necessary, you can change the WAF mode for a virtual service later or deactivate the web application firewall.

After you enable WAF for your virtual service, you can create allowlist rules or edit WAF signatures as needed.

Configure Allowlist Rules for a Virtual Service

You can use the allowlist functionality to define match conditions and associated actions for the WAF to perform when processing a request.

When you create WAF allowlist rules, you instruct the WAF not to apply the WAF policy in specific cases, for example, if the request comes from a specific IP address or range, or if the request matches the URL pattern specified using the HTTP method match type. Configuring allowlist rules can help prevent flooding your logs with false positive WAF violations and reduces latency generated by WAF signature inspections.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway on which the virtual service is configured.

4 Click the virtual service and click **WAF**.

5 Under Allowlist Rules, click **New**.

6 Enter a name for the rule.

7 To activate the rule upon creation, turn on the **Active** toggle.

8 Select match criteria.

Option	Description
Client IP Address	a Select **Is** or **Is Not** to indicate whether to perform an action if the client IP matches or doesn't match the value that you enter. b Enter an IPv4 address, or an IPv6 address, or a range, or a CIDR notation. c (Optional) To add more IP addresses, click **Add IP**.
HTTP Method	a Select **Is** or **Is Not** to indicate whether to perform an action if the HTTP method matches or doesn't match the value that you enter. b From the drop-down menu, select one or more HTTP methods.
Path	a Select a criterion for the path. b Enter a path string. **Note** The path doesn't need to begin with a forward slash (/). c (Optional) To add more paths, click **Add Path**.
Host Header	a Select a criterion for the host header. b Enter a value for the header.

You can add one criterion of each type.

9 Select an action to apply upon a match.

Option	Description
Bypass	The WAF does not execute any further rules and the request is allowed.
Continue	Stops the allowlist execution and proceeds with WAF signature evaluation.
Detection Mode	The WAF evaluates and processes the incoming request, but does not perform a blocking action. A log entry is created when the request is flagged.

10 Click **Add**.

Edit the WAF Signatures for a Virtual Service

You can edit the WAF signatures for a virtial service - you can change a signature mode from **Detection** to **Enforcement** or the reverse, or, if necessary, deactivate a signature or a signature group.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the NSX edge gateway on which the virtual service is configured.

4 Click the virtual service and click **WAF**.

   Under the Signature Groups section, you can see the signature groups that are included in your WAF policy. You can see if they are actively in use or not. You can also see the number or the rules in each group that are active and the number of rules that have been overriden manually.

5 Under Signature Groups, click the expand button on the left of the signature group that you want to edit.

6 To edit the signatures of a group, click **Edit Signatures**.

7 Click the expand button on the left of the signature name and select an action.

8 Click **Save**.

9 To disable a signature group, click the expand button on the left of the signature group and click **Deactivate**.

Managing NSX Data Center for vSphere Edge Gateways in VMware Cloud Director

An NSX Data Center for vSphere edge gateway provides a routed organization virtual data center network with connectivity to external networks and can provide services such as load balancing, network address translation, and a firewall. VMware Cloud Director supports IPv4 and IPv6 edge gateways.

Starting with VMware Cloud Director 9.7, the compute workload and the networking workload are isolated by using different vSphere resource pools and storage policies. Edge gateways reside on edge clusters that you must previously create. See Working with NSX Data Center for vSphere Edge Clusters in VMware Cloud Director.

You can migrate legacy edge gateways to the corresponding edge clusters by redeploying these edge gateways. See Redeploy an Edge Gateway in VMware Cloud Director.

Important Starting with version 9.7, VMware Cloud Director supports only advanced edge gateways. You must convert any legacy non-advanced edge gateway to an advanced gateway. See https://kb.vmware.com/kb/66767.

Working with NSX Data Center for vSphere Edge Clusters in VMware Cloud Director

To isolate the compute workloads from the networking workloads, VMware Cloud Director supports the edge cluster object. An edge cluster consists of a vSphere resource pool and a storage policy that are used only for organization VDC edge gateways. Provider virtual data centers cannot use resources dedicated to edge clusters, and edge clusters cannot use resources dedicated to provider virtual data centers.

Edge clusters provide a dedicated L2 broadcast domain, which reduces the VLAN sprawls and ensures the network security and isolation. For example, the edge cluster can contain additional VLANs for peering with physical routers.

You can create any number of edge clusters. You can assign an edge cluster to an organization VDC as a primary or secondary edge cluster.

- The primary edge cluster for an organization VDC is used for the main edge appliance of an organization VDC edge gateway.
- The secondary edge cluster for an organization VDC is used for the standby edge appliance when an edge gateway is in HA mode.

Different organization VDCs can share edge clusters or can have their own dedicated edge clusters.

Starting with vCloud Director 9.7, the old process for using metadata to control the edge gateway placement is deprecated. See KB article 2151398.

You can migrate legacy edge gateways to newly created edge clusters by redeploying these edge gateways. See Redeploy an Edge Gateway in VMware Cloud Director.

Preparing Your Environment for an Edge Cluster

1. In vSphere, create the resource pool for the target edge cluster.

   If an organization virtual data center is using a VLAN network pool, the VLAN network pool and the edge cluster for this organization virtual data center must reside on the same vSphere distributed switch.

2. If an organization virtual data center is using a VXLAN network pool, in NSX, add the edge cluster to the VXLAN transport zone, after which synchronize the VXLAN network pool in VMware Cloud Director.
3. In vSphere, create the edge cluster storage profile.

Creating and Managing Edge Clusters

After you prepare your environment, to create and manage edge clusters, you must use the VMware Cloud Director OpenAPI `EdgeClusters` methods. See Getting Started with VMware Cloud Director OpenAPI.

Viewing edge clusters requires the **Edge Cluster View** right. Creating, updating, and deleting edge clusters require the **Edge Cluster Manage** right.

When you create an edge cluster, you specify the name, the vSphere resource pool, and the storage profile name.

After you create an edge cluster, you can modify its name and description. After you delete or move its containing edge gateways, you can delete an edge cluster.

Assigning an Edge Cluster to an Organization VDC

After you create an edge cluster, you can assign this edge cluster to an organization VDC by updating the organization VDC network profile. You can assign an edge cluster to an organization VDC as a primary or secondary edge cluster.

If you do not assign a secondary edge cluster, the standby edge appliance of an edge gateway in HA mode is deployed on the primary edge cluster but on a host different from the host running the primary edge appliance.

To update, view, and delete organization VDC network profiles, you must use the VMware Cloud Director OpenAPI `VdcNetworkProfile` methods. See Getting Started with VMware Cloud Director OpenAPI.

Considerations:

- The primary and secondary edge clusters must reside on the same vSphere distributed switch.
- If the organization VDC uses a VXLAN network pool, the NSX Transport Zone must span the compute and the edge clusters.
- If the organization VDC uses a VLAN network pool, the edge clusters and the compute clusters must be on the same vSphere distributed switch.

If you update again the primary or secondary edge cluster of an organization VDC, to move an existing edge gateway to the new cluster, you must redeploy this edge gateway. See Redeploy an Edge Gateway in VMware Cloud Director.

Add an NSX Data Center for vSphere Edge Gateway to VMware Cloud Director

In VMware Cloud Director, an NSX Data Center for vSphere edge gateway provides a routed organization VDC network with connectivity to external networks and can provide services such as load balancing, network address translation, and a firewall.

Starting with VMware Cloud Director 9.7, NSX Data Center for vSphere edge gateways are deployed on edge clusters that you previously created and assigned to the organization VDC.

You can add an IPv4 or IPv6 edge gateway that connects to one or more external networks.

Note IPv6 edge gateways support limited services. IPv6 edge gateways support edge firewalls, distributed firewalls, and static routing.

Prerequisites

- For information about the system requirements for deploying an NSX Data Center for vSphere edge gateway, see the *NSX Administration Guide*.
- If you want to deploy the edge gateway on a dedicated edge cluster, create and assign an edge cluster to the organization virtual data center. See Working with NSX Data Center for vSphere Edge Clusters in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left pane, click **Edge Gateways** and click **New**.

3 Select the NSX-V backed organization virtual data center on which you want to create the edge gateway, and click **Next**.

4 Enter a name and, optionally, a description for the new edge gateway.

5 Turn on or leave turned off each of these general edge gateway settings.

General Setting	Description
Distributed Routing	Configures the edge gateway to provide distributed logical routing.
FIPS Mode	Configures the edge gateway to use NSX FIPS mode.
High Availability	Enables automatic failover to a backup edge gateway.

6 Select the edge gateway configuration for your system resources and click **Next**.

Configuration	Description
Compact	Requires less memory and fewer compute resources.
Large	Provides increased capacity and performance than the Compact configuration. Large and X-Large configurations provide identical security functions.
X-Large	Used for environments that have a load balancer with large numbers of concurrent sessions.
Quad Large	Used for high throughput environments. Requires a high connection rate.

7 Select one or more subnets from the external networks to which the edge gateway can connect, and click **Next**.

If you assigned an edge cluster to the organization VDC, the displayed list contains the external networks that are accessible to this edge cluster.

8 (Optional) Configure a network as the default gateway.

a Turn on the **Configure default gateway** toggle.

b Click the radio button next to the name of the target external network, and click the radio button next to the target IP address.

c (Optional) Turn on the **Use default gateway for DNS Relay** toggle.

9 Click **Next**.

10 Turn on or leave turned off each of these advanced edge gateway settings, and click **Next**.

Advanced Setting	Description
IP Settings	You can manually enter an IP address for each subnet on the edge gateway.
Sub-Allocate IP Pools	You can suballocate multiple static IP pools from the available IP pools of each external network on the edge gateway.
Rate Limits	You can configure the inbound and outbound rate limits for each external network on the edge gateway.

11 (Optional) If you enabled one or more advanced settings in Step 10, configure each enabled setting.

Advanced Setting	Steps
IP Settings	For each network on the edge gateway, in the **IP Addresses** cell, enter an IP address, and click **Next**. If you do not enter an IP address for a network, the system assigns an arbitrary IP address to this network.
Sub-Allocate IP Pools	1 Click the radio button next to the name of an external network and click **Edit**. You can see the available IP pools for this external network and the current suballocated IP pools, if configured. 2 Edit the suballocated IP pools for this external network and click **Save**. You can add IP addresses and ranges from the ranges of the available IP pools. 3 Click **Save**. The system combines overlapping IP ranges. 4 Click **Next**. **Note** Allocating IP addresses to an edge gateway is a process where the provider assigns ownership of IP addresses to the gateway. VMware Cloud Director automatically configures the appropriate gateway interface with the secondary addresses during the allocation process. If any of the IP addresses are used outside of VMware Cloud Director, this can cause IP address conflicts.
Rate limits	For each external network on the edge gateway, turn on the **Enable** toggle, enter the limits in the **Incoming Rate** and **Outgoing Rates** cells, and click **Next**.

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

Configuring NSX Data Center for vSphere Edge Gateway Services in VMware Cloud Director

In VMware Cloud Director, you can configure services such as DHCP, firewall, network address translation (NAT), and VPN on an edge gateway.

Managing an NSX Data Center for vSphere Edge Gateway Firewall in the VMware Cloud Director Service Provider Admin Portal

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 the Distributed Firewall on a VMware Cloud Director Organization Virtual Data Center.

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 activate or deactivate an edge gateway firewall.

Add an NSX Data Center for vSphere Edge Gateway Firewall Rule in the VMware Cloud Director Service Provider Admin Portal

You use the edge gateway **Firewall** tab to add firewall rules for that edge gateway. You can add multiple 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 in the VMware Cloud Director Service Provider Admin Portal

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 in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, and click **Services**.

2 Click the **Firewall** tab.

3 Manage the firewall rules.

   - Deactivate a rule by clicking the green check mark in its **No.** cell. The green check mark turns to a red deactivated icon. If the rule is deactivated and you want to activate the rule, click the red deactivated 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**.

Apply Syslog Server Settings to an NSX Data Center for vSphere Edge Gateway in VMware Cloud Director

If you enabled logging for one or more edge gateway firewall rules, the edge gateway connects to the syslog server. If you created an edge gateway before the initial configuration of the syslog server, or if you changed the syslog server settings, you must synchronize the syslog server settings for this edge gateway.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the radio button next to the name of the target edge gateway, and click **Sync syslog**.
4. To confirm, click **OK**.

Managing NSX Data Center for vSphere Edge Gateway DHCP in the VMware Cloud Director Service Provider Admin Portal

You configure your edge gateways to provide Dynamic Host Configuration Protocol (DHCP) services to VMs connected to the associated organization virtual data center (VDC) networks in VMware Cloud Director.

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 edge gateway which has DHCP activated 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 deactivate and then reactivate DHCP on that edge gateway. See Add a DHCP IP Pool on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Add a DHCP IP Pool on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.

Option	Description
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**.

Results

VMware Cloud Director updates the edge gateway to provide DHCP services.

Add DHCP Bindings To an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.
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 in the VMware Cloud Director Service Provider Admin Portal

You can use the DHCP relay capability that NSX provides in your VMware Cloud Director environment to leverage your existing DHCP infrastructure from within your VMware Cloud 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 in the VMware Cloud Director Service Provider Admin Portal

The NSX software in your VMware Cloud Director environment provides the capability for the edge gateway to relay DHCP messages to DHCP servers external to your VMware Cloud 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 by Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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**.

Add an SNAT or a DNAT Rule To an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 VMware Cloud 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 or select the allocated IP address from the list. 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.
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.
Source IP address	If you want the rule to apply only for traffic from a specific domain, enter an IP address for this domain or an IP address range in CIDR format. If you leave this text box blank, the DNAT rule applies to all IP addresses that are in the local subnet.
Source Port	(Optional) Enter a port number for the source.
Description	(Optional) Enter a meaningful description for the DNAT rule.

Option	Description
Enabled	Toggle on to activate 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, or selet the allocated IP address from the list. 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.
Destination IP Address	(Optional) If you want the rule to apply only for traffic to a specific domain, enter an IP address for this domain or an IP address range in CIDR format. If you leave this text box blank, the SNAT rule applies to all destinations outside of the local subnet.
Destination Port	(Optional) Enter a port number for the destination.
Description	(Optional) Enter a meaningful description for the SNAT rule.
Enabled	Toggle on to activate 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 in the VMware Cloud Director Service Provider Admin Portal.

Advanced Routing Configuration for NSX Data Center for vSphere Edge Gateways in the VMware Cloud Director Service Provider Admin Portal

You can configure the static and dynamic routing on your NSX Data Center for vSphere 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 Data Center for vSphere provides, see the NSX Data Center for vSphere 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 Data Center for vSphere 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 in the VMware Cloud Director Service Provider Admin Portal

You can specify the default settings for static routing and dynamic routing for an edge gateway in VMware Cloud Director.

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 To an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Configure route redistribution. See Configure Route Redistributions on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Configure dynamic routing. See the following topics:

- Configure BGP On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal
- Configure OSPF On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

Add a Static Route To an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

You can add a static route for a destination subnet or host in VMware Cloud Director.

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 in the VMware Cloud Director Service Provider Admin Portal 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.
   - b In the left panel, click **Edge Gateways**.
   - c Click the radio button next to the name of the target edge gateway, 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 an SNAT or a DNAT Rule To an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Add a firewall rule to allow traffic to traverse the static route. See Add an NSX Data Center for vSphere Edge Gateway Firewall Rule in the VMware Cloud Director Service Provider Admin Portal.

Configure OSPF On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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 VMware Cloud Director environment is to exchange routing information between edge gateways in VMware Cloud 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 in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 in the VMware Cloud Director Service Provider Admin Portal.

Make sure that the route redistribution and firewall configuration allow the correct routes to be advertised. See Configure Route Redistributions on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Configure BGP On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.

Option	Description
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.
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 in the VMware Cloud Director Service Provider Admin Portal for information.

Configure Route Redistributions on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

By default the router only shares routes with other routers running the same protocol. When you have configured a multi-protocol VMware Cloud Director 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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**.

About Load Balancing with NSX Data Center for vSphere in VMware Cloud Director

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 use, maximizing throughput, minimizing response time, and avoiding overload.

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 NSX Data Center for vSphere 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 the 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 back end servers.

Server Pool Member

Represents the back end 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 can use an 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 Load Balancing On NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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.
    1. From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.
    2. In the left panel, click **Edge Gateways**.
    3. Click the radio button next to the name of the target edge gateway, 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**.

What to do next

Configure application profiles for the load balancer. See Create an Application Profile On An NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Create an Application Profile On An NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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) Enter the URL to which traffic that arrives at the destination address should be redirected.
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. ■ **SSL Session ID** SSL Session ID persistence is available when you enable SSL passthrough. SSL Session ID persistence ensures that repeat connections from the same client are sent to the same server. Session ID persistence allows the use of SSL session resumption, which saves processing time for both the client and the server.
Cookie Name	(HTTP and HTTPS) If you specified **Cookie** as the persistence mechanism, enter 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.

Option	Description
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.
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. **Note** Using this header is not supported if you enabled SSL passthrough.
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.

Option	Description
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 To preserve your changes, click **Keep**.

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 On An NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Create a Service Monitor On An NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.

Option	Description
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 activated or deactivated.
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 To preserve your changes, click **Keep**.

Example: Extensions Supported for Each Protocol

Table 5-1. 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.

Table 5-1. Extensions for HTTP/HTTPS Protocols (continued)

Monitor Extension	Description
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 5-2. 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 5-3. 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`.

Table 5-3. Extensions for TCP Protocol (continued)

Monitor Extension	Description
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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Add a Server Pool for Load Balancing On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 To preserve your changes, click **Keep**.

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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Add an Application Rule On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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/2.2/configuration.html.

6 To preserve your changes, click **Keep**.

What to do next

Associate the new application rule to a virtual server added for the load balancer. See Add a Virtual Server On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Add a Virtual Server On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

Add an NSX Data Center for vSphere edge gateway internal or uplink interface as a virtual server in VMware Cloud Director. 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

6. To preserve your changes, click **Keep**.

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 in the VMware Cloud Director Service Provider Admin Portal

Configure Secure Access Using VPN on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can configure the VPN capabilities that are provided by the NSX Data Center for vSphere software on your NSX Data Center for vSphere edge gateways in VMware Cloud Director. 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 VMware Cloud 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 VMware Cloud 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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

The SSL VPN-Plus services for an NSX Data Center for vSphere edge gateway in your VMware Cloud 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 VMware Cloud 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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal 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 on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal.

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 on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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 in VMware Cloud Director.

2. Configure SSL VPN Server Settings on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

   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 NSX Data Center for vSphere edge gateway in VMware Cloud Director, 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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 in the VMware Cloud Director Service Provider Admin Portal.

4 Add a Private Network for Use with SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   Use the Private Networks screen on the **SSL VPN-Plus** tab to configure the private networks in the VMware Cloud Director Service Provider Admin Portal. 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 activated private networks will be installed in the routing table of the VPN client.

5 Configure an Authentication Service for SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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. VMware Cloud Director uses this authentication server 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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

   To add accounts for your remote users to the local authentication server for the NSX Data Center for vSphere edge gateway SSL VPN service, use the **Users** screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

7 Add an SSL VPN-Plus Client Installation Package On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

   To create named installation packages of the SSL VPN-Plus client for the remote users, use the Installation Packages screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

8 Edit the SSL VPN-Plus Client Configuration On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

   To customize the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN, use the **Client Configuration** screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

9 Customize the General SSL VPN-Plus Settings for an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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

Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 in VMware Cloud Director.

Procedure

1. Open Edge Gateway Services.

   a. From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b. In the left panel, click **Edge Gateways**.

   c. Click the radio button next to the name of the target edge gateway, 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Configure SSL VPN Server Settings on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

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 NSX Data Center for vSphere edge gateway in VMware Cloud Director, 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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

- 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 Using Your VMware Cloud Director Service Provider Admin Portal.

- Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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 activated by default. You can change the level of messages to log or deactivate 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 in the VMware Cloud Director Service Provider Admin Portal.

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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Create an IP Pool for Use with SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 in the VMware Cloud Director Service Provider Admin Portal.

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 Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Configure SSL VPN Server Settings on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

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 activate or deactivate 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**.

Results

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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Add a Private Network for Use with SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

Use the Private Networks screen on the **SSL VPN-Plus** tab to configure the private networks in the VMware Cloud Director Service Provider Admin Portal. 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 activated 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 activate 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 deactivate TCP optimization for that private network. Also, the private network for that FTP server must be activated and appear in the on-screen table above the TCP-optimized private network.

Prerequisites

- Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Create an IP Pool for Use with SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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 activated edge gateway. ■ **Bypass Tunnel** The VPN client bypasses the edge gateway and sends the traffic directly to the private server.
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 activate 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	Activate or deactivate 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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 in the VMware Cloud Director Service Provider Admin Portal.

Configure an Authentication Service for SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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. VMware Cloud Director uses this authentication server 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 Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Add a Private Network for Use with SSL VPN-Plus on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- 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 Using Your VMware Cloud Director Service Provider Admin Portal.

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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

To add accounts for your remote users to the local authentication server for the NSX Data Center for vSphere edge gateway SSL VPN service, use the **Users** screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Prerequisites

Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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 activated or deactivated.
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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

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 On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Add an SSL VPN-Plus Client Installation Package On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

To create named installation packages of the SSL VPN-Plus client for the remote users, use the Installation Packages screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

You can add an SSL VPN-Plus client installation package to the NSX Data Center for vSphere 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 Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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.
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 activated or deactivated.

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.

Option	Description
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 the SSL VPN-Plus Client Configuration On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal.

Edit the SSL VPN-Plus Client Configuration On an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal

To customize the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN, use the **Client Configuration** screen on the **SSL VPN-Plus** tab in the VMware Cloud Director Service Provider Admin Portal.

Prerequisites

Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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) Deactivate auto reconnect.

Enable auto reconnect is activated by default. If auto reconnect is activated, 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 deactivated by default. If you activate this option, remote users can choose to install the upgrade.

6 Click **Save changes**.

Customize the General SSL VPN-Plus Settings for an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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

Prerequisites

Navigate to the SSL-VPN Plus Screen Of an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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.
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 on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

The NSX Data Center for vSphere edge gateways in a VMware Cloud 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 (AES256-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 on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   Use the **IPsec VPN Sites** screen in the VMware Cloud 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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 on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

   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 on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Configure the IPsec VPN Site Connections for the NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

Use the **IPsec VPN Sites** screen in the VMware Cloud 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 VMware Cloud 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 on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- Configure IPsec VPN on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

- 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 on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 On the **IPsec VPN** tab, click **IPsec VPN Sites**.

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

3 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.

4 Click **Keep**.

5 Click **Save changes**.

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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Enable the IPsec VPN Service on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.
- 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

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**.

Results

The edge gateway IPsec VPN service is active.

Specify Global IPsec VPN Settings on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

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 Using Your VMware Cloud Director Service Provider Admin Portal.
- Navigate to the IPsec VPN Screen on an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Configure L2 VPN in the VMware Cloud Director Service Provider Admin Portal

The NSX Data Center for vSphere edge gateways in a VMware Cloud 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.

Procedure

1 Navigate to the L2 VPN Screen Using Your VMware Cloud Director Service Provider Admin Portal

   To begin configuring the L2 VPN service for an NSX Data Center for vSphere edge gateway in VMware Cloud Director, you must navigate to the **L2 VPN** screen.

2 Configure the NSX Data Center for vSphere Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal

   The L2 VPN server is the destination NSX edge to which the L2 VPN client is going to connect.

3 Configure the NSX Data Center for vSphere Edge Gateway as an L2 VPN Client in the VMware Cloud Director Service Provider Admin Portal

   The L2 VPN client is the source NSX edge that initiates communication with the destination NSX edge, the L2 VPN server.

4 Enable the L2 VPN Service on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

   When the required L2 VPN settings are configured, you can enable the L2 VPN service on the edge gateway.

Navigate to the L2 VPN Screen Using Your VMware Cloud Director Service Provider Admin Portal

To begin configuring the L2 VPN service for an NSX Data Center for vSphere edge gateway in VMware Cloud Director, you must navigate to the **L2 VPN** screen.

Procedure

1. Open Edge Gateway Services.
   1. From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.
   2. In the left panel, click **Edge Gateways**.
   3. Click the radio button next to the name of the target edge gateway, and click **Services**.
2. Navigate to **VPN > L2 VPN**.

What to do next

Configure the L2 VPN server. See Configure the NSX Data Center for vSphere Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal.

Configure the NSX Data Center for vSphere Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal

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 Using Your VMware Cloud Director Service Provider Admin Portal.
- 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 Using Your VMware Cloud Director Service Provider Admin Portal.
- 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.

Option	Action
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) Enter 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**.

What to do next

Enable the L2 VPN service on this edge gateway. See Enable the L2 VPN Service on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal.

Configure the NSX Data Center for vSphere Edge Gateway as an L2 VPN Client in the VMware Cloud Director Service Provider Admin Portal

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 Using Your VMware Cloud Director Service Provider Admin Portal.

- 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 Using Your VMware Cloud Director Service Provider Admin Portal.

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**.

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.
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**.

What to do next

Enable the L2 VPN service on this edge gateway. See Enable the L2 VPN Service on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal.

Enable the L2 VPN Service on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

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 NSX Data Center for vSphere Edge Gateway as an L2 VPN Server in the VMware Cloud Director Service Provider Admin Portal.
- 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 NSX Data Center for vSphere Edge Gateway as an L2 VPN Client in the VMware Cloud Director Service Provider Admin Portal.
- Navigate to the L2 VPN Screen Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 On the **L2 VPN** tab, click the **Enable** toggle.

2 Click **Save changes**.

Results

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 NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

You can remove the existing L2 VPN service configuration of the edge gateway. This action also deactivates the L2 VPN service on the edge gateway.

Prerequisites

Navigate to the L2 VPN Screen Using Your VMware Cloud Director Service Provider Admin Portal

Procedure

1. Scroll down to the bottom of the L2 VPN screen, and click **Delete configuration**.
2. To confirm the deletion, click **OK**.

Results

The L2 VPN service is deactivated and the configuration details are removed from the edge gateway.

SSL Certificate Management on an NSX Data Center for vSphere Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

The NSX Data Center for vSphere software in the VMware Cloud 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 VMware Cloud Director environment support self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA. You 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 VMware Cloud 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 Data Center for vSphere 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 Using Your VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 VMware Cloud 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	Enter 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. When FIPS mode is on, RSA key sizes must be greater or equal to 2048 bits. **Note** SSL VPN-Plus supports RSA certificates only.

Option	Description
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.

Results

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 Using Your VMware Cloud Director Service Provider Admin Portal.
- Use the CSR to create a self-signed certificate. See Configure a Self-Signed Service Certificate Using Your VMware Cloud Director Service Provider Admin Portal.

Import the CA-Signed Certificate Corresponding to the CSR Generated for an Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

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 in VMware Cloud Director.

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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) Enter 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.

Results

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 on an NSX Data Center for vSphere Edge Gateway Using the VMware Cloud Director Service Provider Admin Portal and Specify Global IPsec VPN Settings on an NSX Edge Gateway in the VMware Cloud Director Service Provider Admin Portal.

Configure a Self-Signed Service Certificate Using Your VMware Cloud Director Service Provider Admin Portal

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 Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 Enter 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.

Results

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 Using Your VMware Cloud Director Service Provider Admin Portal

Adding a CA certificate to an edge gateway in VMware Cloud Director 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 Using Your VMware Cloud Director Service Provider Admin Portal.

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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) Enter a description.

6 Click **Keep**.

Results

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 Using Your VMware Cloud Director Service Provider Admin Portal

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 to VMware Cloud Director. 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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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) Enter a description.

6 Click **Keep**.

Results

The CRL appears in the on-screen list.

Add a Service Certificate to the Edge Gateway Using Your VMware Cloud Director Service Provider Admin Portal

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 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.

   When FIPS mode is on, RSA key sizes must be greater or equal to 2048 bits.

   - 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) Enter a description.

8 Click **Keep**.

Results

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 for NSX Data Center for vSphere Edge Gateways in the VMware Cloud Director Service Provider Admin Portal

The NSX Data Center for vSphere software in your VMware Cloud 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 by Using Your VMware Cloud Director Service Provider Admin Portal

An IP set is a group of IP addresses that you can create at a VMware Cloud Director 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. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

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 To save this IP set, click **Keep**.

Results

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 by Using Your VMware Cloud Director Service Provider Admin Portal

A MAC set is a group of MAC addresses that you can create at an organization virtual data center level in VMware Cloud Director. You can use a MAC set as the source or destination in a firewall rule.

You create a MAC set by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

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 To save the MAC set, click **Keep**.

Results

The new MAC set is available for selection as the source or destination in firewall rules.

View Services Available for Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

2 Click the **Services** tab.

Results

The available services are displayed on the screen.

View Service Groups Available for Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

2 Click the **Service Groups** tab.

Results

The available service groups are displayed on the screen. The Description column displays the services that are grouped in each service group.

View the Networks Use and IP Allocations on an NSX Data Center for vSphere Edge Gateway in VMware Cloud Director

You can view the networks on an edge gateway with information about their IP pool use and subnets. You can also view the IP address allocated to each network.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 To view the external networks with information about their IP pool use and subnets, click the **External Networks > Networks & subnets** tab.

4 To view the external networks with information about their IP addresses and categories, click the **External Networks > IP allocations** tab.

Editing NSX Data Center for vSphere Edge Gateway Properties in VMware Cloud Director

Activate or Deactivate Distributed Routing on an Edge Gateway in VMware Cloud Director

After you activate VMware Cloud Director distributed routing on an edge gateway, the organization administrator can create many routed organization virtual data center networks with distributed interfaces connected to this edge gateway. Traffic on those networks is optimized for VM-to-VM communication.

Prerequisites

The backing NSX-V Manager instance is configured with an NSX Controller cluster. See the *NSX Administration Guide*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Select the radio button next to the name of the target edge gateway, and click **Enable distributed routing** or **Disable distributed routing**.

4 To confirm, click **OK**.

Modify the External Networks and the Edge Gateway Settings in VMware Cloud Director

To modify the external networks and the edge gateway settings in VMware Cloud Director, you can use the **Edit edge gateway** wizard, which contains the same pages as the wizard that you used to create the edge gateway.

You can modify the settings that you configured when adding the edge gateway. See Add an NSX Data Center for vSphere Edge Gateway to VMware Cloud Director.

To modify the distributed routing setting, see Activate or Deactivate Distributed Routing on an Edge Gateway in VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**.
3. Click the radio button next to the name of the edge gateway that you want to modify, and click **Edit**.
4. To modify the edge gateway settings, go through the pages of the **Edit edge gateway** wizard by clicking **Next**, and, on the **Ready to Complete** page, click **Finish**.

Edit the General Settings of an Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can modify the name and the description of an edge gateway, activate or deactivate FIPS mode and high availability state, and change the edge gateway size configuration.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.
3. On the **General** tab, in the upper-right corner, click **Edit**.
4. (Optional) Edit the name and the description of the edge gateway.
5. (Optional) Turn on or off each general edge gateway settings.

General Setting	Description
FIPS Mode	Configures the edge gateway to use NSX FIPS mode.
High Availability	Activates automatic failover to a backup edge gateway.

6 (Optional) Change the edge gateway configuration for your system resources.

Configuration	Description
Compact	Requires less memory and fewer compute resources.
Large	Provides increased capacity and performance than the Compact configuration. Large and X-Large configurations provide identical security functions.
X-Large	Used for environments that have a load balancer with large numbers of concurrent sessions.
Quad Large	Used for high throughput environments. Requires a high connection rate.

7 To confirm the changes, click **Save**.

Edit the Default Gateway of an Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can change the network that an edge gateway uses as a default gateway.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 On the **External Networks > Default gateway** tab, in the upper-right corner, click **Edit**.

4 (Optional) Configure a network as the default gateway.

   a Turn on the **Configure default gateway** toggle.

   b Select the radio button next to the name of the target external network, and select the radio button next to the target IP address.

   c (Optional) Turn on the **Use default gateway for DNS Relay** toggle.

5 To confirm the changes, click **Save**.

Edit the IP Settings of an Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can modify the IP settings for external networks on an edge gateway.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 On the **External Networks > IP settings** tab, click **Edit**.

4 For each network on the edge gateway, in the **IP Addresses** cell, enter an IP address or leave the cell blank.

   If you do not enter an IP address for a network, the system assigns an arbitrary IP address to this network.

5 To confirm the changes, click **Save**.

Edit the Suballocated IP Pools on an Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can suballocate multiple static IP pools from the available IP pools of an external network on an edge gateway.

Note Allocating IP addresses to an edge gateway through sub-allocation is a process where the provider assigns ownership of IP addresses to the gateway. VMware Cloud Director automatically configures the appropriate gateway interface with the secondary addresses during the sub-allocation process, which can cause IP address conflicts if any of the IP addresses are used outside of VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 Click the **External Networks > Sub-allocated IP pools** tab.

   You can see the current suballocated IP pools for each external network on this edge gateway.

4 Click the radio button next to the name of an external network, and click **Edit**.

   You can see the available IP pools for this external network, and the current suballocated IP pools if configured.

5 Edit the suballocated IP pools for this external network, and click **Save**.

   You can add, modify, and remove IP addresses and ranges from the ranges of the available IP pools.

Results

The system combines overlapping IP ranges.

Edit the Rate Limits on an Edge Gateway in VMware Cloud Director

In VMware Cloud Director, you can configure the inbound and outbound rate limits for each external network on the edge gateway.

Rate limits apply only to external networks backed by distributed port groups with static binding.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**, and click the name of the target edge gateway.

3 On the **External Networks > Rate limits** tab, in the upper-right corner, click **Edit**.

   You can see the current rate limits for each external network on this edge gateway.

4 Edit the rate limits, and click **Save**.

   For each external network on the edge gateway, you can activate or deactivate the rate limits, and you can change the incoming and outgoing rates.

Redeploy an Edge Gateway in VMware Cloud Director

You can delete and deploy a new edge gateway appliance with the latest configurations.

If edge services are not working as expected, you can redeploy the edge gateway appliance.

When you redeploy an edge gateway, VMware Cloud Director deletes it and recreates it with the latest configurations.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the radio button next to the name of the target edge gateway, and click **Redeploy**.

4 To confirm, click **OK**.

Results

The edge gateway virtual machine is replaced with a new virtual machine and all services are restored.

Delete an Edge Gateway From VMware Cloud Director

You can remove an edge gateway from the VMware Cloud Director organization virtual data center.

Prerequisites

Delete all organization virtual data center networks that use the target edge gateway.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Edge Gateways**.

3 Click the radio button next to the name of the target edge gateway, and click **Delete**.

4 To confirm, click **Delete**.

Statistics and Logs for an NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can view statistics and logs for an NSX Data Center for vSphere edge gateway.

View Statistics in the VMware Cloud Director Service Provider Admin Portal

You can view statistics on the **Edge Gateway Services** screen.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 for the firewall. 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 in the VMware Cloud Director Service Provider Admin Portal

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

- Verify that your role includes the **Configure System Logging** right.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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 VMware Cloud Director system administrator has already configured a Syslog server for the VMware Cloud 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 NSX Data Center for vSphere Edge Gateway in the VMware Cloud Director Service Provider Admin Portal

You can enable SSH command-line access to an edge gateway.

Procedure

1 Open Edge Gateway Services.

   a From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

   b In the left panel, click **Edge Gateways**.

   c Click the radio button next to the name of the target edge gateway, 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.

Managing Provider Virtual Data Centers in Your VMware Cloud Director

6

After you create a provider virtual data center in VMware Cloud Director, you can modify its properties, deactivate or delete it, and manage its storage policies and resource pools.

To create a provider virtual data center, you must use either the Service Provider Admin Portal or the vCloud API. For information about using Service Provider Admin Portal, see Create a Provider Virtual Data Center in Your VMware Cloud Director. For information about using the vCloud API, see the *VMware Cloud Director API Programming Guide*.

Read the following topics next:

- Activate or Deactivate a Provider Virtual Data Center in Your VMware Cloud Director
- Delete a Provider Virtual Data Center in Your VMware Cloud Director
- Edit the General Settings of a Provider Virtual Data Center in Your VMware Cloud Director
- Merge Provider Virtual Data Centers in Your VMware Cloud Director
- View the Organization Virtual Data Centers of a Provider Virtual Data Center in Your VMware Cloud Director
- View the Datastores and Datastore Clusters on a Provider Virtual Data Center in Your VMware Cloud Director
- Configure Low Disk Space Thresholds for a Provider Virtual Data Center Storage Container in Your VMware Cloud Director
- View the External Networks on a Provider Virtual Data Center in Your VMware Cloud Director
- Using Kubernetes with Your VMware Cloud Director
- Managing the VM Storage Policies on a Provider Virtual Data Center in Your VMware Cloud Director
- Managing the Resource Pools on a VMware Cloud Director Provider Virtual Data Center
- Modify the Metadata for a VMware Cloud Director Provider Virtual Data Center

Activate or Deactivate a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, to deactivate all existing organization virtual data centers (VDCs) that use the resources of a provider VDC, you can deactivate this provider VDC. You cannot create organization VDCs that use the resources of a deactivated provider VDC.

Running vApps and powered on virtual machines continue to run in the existing organization VDCs backed by this provider VDC, but you cannot create or start additional vApps or virtual machines.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click the radio button next to the name of the target provider VDC, and click **Enable** or **Disable**.
4. To confirm, click **OK**.

Delete a Provider Virtual Data Center in Your VMware Cloud Director

To remove the resources of a provider virtual data center from VMware Cloud Director, you can delete this provider virtual data center.

The underlying resources in vSphere remain unaffected.

Prerequisites

- Deactivate the target provider virtual data center. See Activate or Deactivate a Provider Virtual Data Center in Your VMware Cloud Director.
- Delete all organization virtual data centers that use resources from this provider virtual data center. See Delete an Organization Virtual Data Center From VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click the radio button next to the name of the provider virtual data center that you want to remove, and click **Delete**.
4. To confirm, click **OK**.

Edit the General Settings of a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, you can change the name and the description of a provider virtual data center. If the backing resource pool supports a higher virtual hardware version, you can upgrade the highest virtual hardware supported by a provider virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Provider VDCs**, and click the name of the provider virtual data center that you want to modify.

3 On the **Configure > General** tab, in the upper right corner, click **Edit**.

4 (Optional) Modify the name and the description of the provider virtual data center.

5 (Optional) Enter a compute provider scope for the provider virtual data center.

   The compute provider scope represents compute fault domains, or availability zones which are visible to tenants and where workloads reside. By default, the compute provider scope of a provider virtual data center is inherited from the backing vCenter Server instance. You can differentiate the compute provider scope for the different provider VDCs that are backed by a single vCenter Server instance. For example, you can set the vCenter Server with a compute provider scope `Germany` and you can set the provider VDC with a scope `Munich`.

6 (Optional) From the drop-down menu, select the highest hardware version supported by this provider virtual data center, and click **Save**.

   The highest version that you can select depends on the ESXi hosts in the resource pool that backs the provider virtual data center.

   Note You can only upgrade the hardware version supported by a provider virtual data center. You cannot downgrade the hardware version. VMware Cloud Director supports the highest hardware version that the backing vSphere infrastructure supports. You can set the hardware version without manually configuring the default hardware version in the vCenter Server instance.

7 Click **Save**.

Merge Provider Virtual Data Centers in Your VMware Cloud Director

To combine the resources of two VMware Cloud Director provider VDCs, you can merge these provider VDCs into a single provider VDC.

You can merge provider VDCs that are backed by NSX.

VMware Cloud Director supports merging provider VDCs that are not backed by networking resources, and merging a provider VDC that is not backed by networking resources with an NSX-backed provider VDC.

Prerequisites

- Verify that both provider VDCs have the same enabled state.
- If you want to merge provider VDCs that are backed by NSX, verify that both provider VDCs are backed by the same NSX Manager instance and by the same Geneve network pool.
- Verify that both provider VDCs are backed by the same vCenter Server instance and by the same data center.
- Verify that the provider VDC that you want to expand supports the highest hardware version used in the provider VDC that is to be merged. If the merging provider VDC contains a VM with a higher hardware version than the highest one supported by the expanding provider VDC, the merge fails.
- Verify that both provider VDCs contain only elastic organization VDCs.
- If you want to merge provider VDCs with network pools that are backed by VXLAN, verify that the VXLAN pools have the same NSX working state. See "Verify the NSX Working State" in the *NSX Upgrade Guide*.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Select the provider virtual data center that you want to expand, and click **Merge**.
4. Select the provider virtual data center to merge with the target provider VDC, and click **Merge**.

View the Organization Virtual Data Centers of a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, you can view a list of the organization virtual data centers that are using resources from a provider virtual data center.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Click the **Organization VDCs** tab.

Results

The list of the organization virtual data centers that are consuming the resources from this provider virtual data center displays. For each organization VDC, the list includes information about the status, state, allocation model, organization, vCenter Server instance, number of networks, number of vApps, number of storage policies, and number of resource pools.

What to do next

- You can go the organization virtual data center view in the VMware Cloud Director Tenant Portal by clicking the **pop-out** icon (↗) next to the name of the target organization virtual data center.
- By clicking the radio button next to the name of an organization virtual data center, you can perform management operations that are similar to the operations described in Chapter 8 Managing Organization Virtual Data Centers in VMware Cloud Director.

View the Datastores and Datastore Clusters on a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, you can view details about the datastores and datastore clusters that provide the storage capacity to a provider virtual data center (VDC).

To see the list of storage containers for all provider VDCs, navigate to **Storage Containers** under the **Infrastructure Resources** tab.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Select the **Storage Containers** tab.

   A list of all datastores and datastore clusters on the provider virtual data center appears. The list contains the following information for each container type.

Title	Description
Name	The name of the datastore
State	Activated or deactivated
Type	The type of file system that the datastore uses, such as Virtual Machine File System (VMFS), Network File System (NFS), vSphere Virtual Volumes, or vSAN datastores.
Used	The datastore space occupied by virtual machine files, including log files, snapshots, and virtual disks. When a virtual machine is powered on, the used hard disk space also includes log files.

Title	Description
Provisioned	The datastore space guaranteed to virtual machines. If any virtual machines are using thin provisioning, some of the provisioned space might not be in use, and other virtual machines can occupy the unused space. This value might be larger than the actual datastore capacity if thin provisioning is used.
Requested	Provisioned storage in use only by VMware Cloud Director objects on the datastore, including: ■ Virtual machines provisioned in VMware Cloud Director ■ Catalog items (templates and media) ■ NSX Edges ■ Used and unused memory swap requirements for virtual machines This value does not include storage requested by shadow VMs or intermediate disks in a linked clone tree.
Threshold Yellow	You receive an email from VMware Cloud Director when the datastore or datastore cluster reaches a specific threshold of unused capacity. By default, VMware Cloud Director sets the yellow threshold to 25% of the stand-alone datastore or datastore cluster's total capacity.
Threshold Red	You receive an email from VMware Cloud Director when the datastore or datastore cluster reaches a specific threshold of unused capacity. By default, VMware Cloud Director sets the red threshold to 15% of the stand-alone datastore or datastore cluster's total capacity. When a datastore reaches its red threshold, the virtual machine placement engine stops placing new virtual machines on the datastore except for already-placed imported VMs.
vCenter Server Name	The vCenter Server instance associated with the datastore.

4 (Optional) To see a list of the datastores in a datastore cluster, select the Datastore Cluster container type and select the **Datastores** tab.

What to do next

To edit the storage container thresholds, see Configure Low Disk Space Thresholds for a Provider Virtual Data Center Storage Container in Your VMware Cloud Director

Configure Low Disk Space Thresholds for a Provider Virtual Data Center Storage Container in Your VMware Cloud Director

You can configure low disk space thresholds on a storage container to receive an email from VMware Cloud Director when the datastore reaches a specific threshold of available capacity. These warnings alert you to a low disk situation before it becomes a problem.

There are two datastore thresholds in VMware Cloud Director.

- Red threshold - the amount of free space on a datastore, below which, VMware Cloud Director filters out the datastore during the placement of any entity such as a VM, a template, or a disk.

  When a datastore reaches its red threshold, the workload placement engine stops placing new VMs on the datastore except while importing VMs from vCenter Server. In the case of VM import, if the vCenter Server VM is already present on the red threshold datastore, the placement engine prefers the existing datastore.

  The workload placement engine uses the red threshold for all workflows. When making a request for any new placement, the placement engine first filters out any datastores or storage pods which have breached the red threshold. When making a placement request for an existing entity, if the disks are residing on the datastores that are breaching the red threshold, VMware Cloud Director relocates the disks to other available datastores. Then, the engine selects a datastore out of the remaining datastores or storage pods, either through the selector logic of VMware Cloud Director or from the vSphere Storage DRS recommendations.

- Yellow threshold - the amount of free space on the datastore, below which VMware Cloud Director filters out the datastore during the placement of shadow VMs from which VMware Cloud Director creates fast-provisioned VMs. For more information on shadow VMs, see Fast Provisioning of Virtual Machines.

  The yellow threshold does not apply to the linked clones that VMware Cloud Director uses for fast provisioning of VMs. When the placement engine selects a datastore for a linked clone, if the selected datastore is missing a shadow VM, VMware Cloud Director creates a shadow VM on the datastore. The threshold does not apply to the shadow VM in this case.

  The yellow threshold applies only to the periodic background job creating shadow VMs. If activated, the job runs every 24 hours and uses eager VM creation on each datastore for a given hub and storage policy pair. To activate the job for eager provisioning of shadow VMs, you must set the following property to `true`.

  ```
  valc.catalog.fastProvisioning=true
  ```

  Note The periodic background job creates shadow VMs on all datastores for all templates. The job increases the storage consumption even when you are not using the datastores or shadow VMs.

When implementing the threshold logic, VMware Cloud Director does not evaluate the requirements of the current placement subject. For the workload placement engine to place a subject on a datastore, the available space in bytes must be more than the threshold in bytes. For example, for a datastore with available capacity of 5 GB with a red threshold set at 4 GB, the placement engine can place a VM with a requirement for 2 GB. If the VM creation breaches the threshold, the placement engine filters out the datastore for further placements.

When you set thresholds on a stand-alone datastore, they apply only to that datastore. If you set thresholds on a datastore cluster, they apply to all datastores in the cluster. By default, VMware Cloud Director sets the red threshold to 15% and the yellow threshold to 25% of the stand-alone datastore or the datastore cluster's total capacity.

Because the default thresholds on a datastore cluster are based on the total cluster capacity, the thresholds might exceed the capacity of individual datastores within the cluster. When setting thresholds on a datastore cluster, consider the capacity of each datastore in the cluster and set thresholds manually rather than accepting the default threshold configurations.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Select the **Storage Containers** tab.
4. Click the name of a storage container and click **Edit**.
5. Select the disk space thresholds for the storage container.
6. Click **Save**.

Results

VMware Cloud Director sets the thresholds for all provider virtual data centers that use the datastore. VMware Cloud Director sends an email alert when the datastore crosses the threshold. When a datastore reaches its red threshold, the virtual machine placement engine stops placing new virtual machines on the datastore except for already-placed imported VMs.

View the External Networks on a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, you can view a list of the external networks that are accessible to a provider virtual data center.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Click the **External Networks** tab.

Results

You can view a list of the available external networks with information about their gateway CIDR settings and IP pool use.

Using Kubernetes with Your VMware Cloud Director

By using Kubernetes with VMware Cloud Director, you can provide a multi-tenant Kubernetes service to your tenants.

For tenant information on working with Kubernetes clusters, see Working with Kubernetes Clusters in the VMware Cloud Director Tenant Portal.

VMware Cloud Director Container Service Extension

Kubernetes Container Clusters is the VMware Cloud Director Container Service Extension plug-in for VMware Cloud Director. To create Kubernetes clusters, service providers and tenants must use the Kubernetes Container Clusters plug-in. You can download the latest compatible Kubernetes Container Clusters plug-in from the VMware Cloud Director download page for the relevant VMware Cloud Director version, and upload the plug-in to the VMware Cloud Director Service Provider Admin Portal. To enable tenants to create Kubernetes clusters, you must publish the plug-in to the tenant organizations. For more information, see VMware Cloud Director Container Service Extension Documentation.

vSphere with Tanzu in VMware Cloud Director

You can use vSphere with Tanzu in VMware Cloud Director to create provider virtual data centers (VDCs) backed by Supervisor Clusters. A host cluster with enabled vSphere with Tanzu is called a Supervisor Cluster. You can set restrictions on the uses of the resources and limit the available resources, including number of Kubernetes clusters per organization, user, or group. For more information, see Manage Quotas on the Resource Consumption of an Organization in VMware Cloud Director.

To use vSphere with Tanzu in VMware Cloud Director, first, you must enable the vSphere with Tanzu functionality on a vSphere 7.0 or later cluster, and configure that cluster as a Supervisor Cluster. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation. The vCenter Server instance that you want to use can have both host clusters and Supervisor Clusters.

To create clusters, you must publish a provider VDC Kubernetes policy to an organization and apply the organization VDC Kubernetes policy during the creation.

VMware Tanzu® Kubernetes Grid™ Service Clusters

VMware Tanzu® Kubernetes Grid™ Service clusters, informally known as TKGS - You can use the vSphere with Tanzu runtime option to create vSphere with Tanzu managed Tanzu Kubernetes Grid Service clusters. Tanzu Kubernetes Grid Service supports VMware hardened and signed upstream compatible Kubernetes, multiple control plane nodes, First Class Disk-based dynamic and static provisioning of Persistent Volumes, and L4 load balancer automation. This option offers more features, however, it might be more expensive. For more information, see the *vSphere with Tanzu Configuration and Management* guide in the vSphere documentation.

Important To integrate Tanzu Kubernetes Grid Service with VMware Cloud Director, when configuring the supervisor cluster in vSphere, you must configure the NSX option.

Workflow for Tanzu Kubernetes Cluster Creation

1 Add a vCenter Server 7.0 or later instance with an enabled vSphere with Tanzu functionality to VMware Cloud Director. See Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director.

2 Verify the network settings on each Supervisor Cluster to enable them to run Kubernetes workloads.

   Important The IP address ranges for the `Ingress CIDRs` and `Services CIDR` parameters must not overlap with IP addresses 10.96.0.0/12 and 192.168.0.0/16 which are the default vSphere values for the `services` and `pods` parameters. See the configuration parameters for Tanzu Kubernetes clusters information in the *vSphere with Kubernetes Configuration and Management* guide.

   Note If you modify the network settings of the Supervisor Cluster after the initial setup, you must refresh the vCenter Server instance to adjust the automatic firewall policies and NAT rules that block the access to the Tanzu Kubernetes cluster from outside the organization virtual data center in which the cluster is created.

3 Create a provider VDC backed by a Supervisor Cluster. See Create a Provider Virtual Data Center in Your VMware Cloud Director.

   Alternatively, you can add a Supervisor Cluster to an existing provider VDC. If you have a vSphere 6.7 or earlier environment, you can also upgrade the environment to version 7.0 and enable vSphere with Tanzu on an existing cluster.

   Provider VDCs backed by a Supervisor Cluster appear with a Kubernetes icon next to their name in the grid that lists all provider VDCs.

4 (Optional) VMware Cloud Director generates automatically a default provider VDC Kubernetes policy for provider VDCs backed by a Supervisor Cluster. You can create additional provider VDC Kubernetes policies for Tanzu Kubernetes clusters. See Create a Provider VDC Kubernetes Policy in Your VMware Cloud Director.

5 Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director from the **Provider VDCs** tab or Add an Organization VDC Kubernetes Policy in VMware Cloud Director from the **Organization VDCs** tab.

6 Publish the Kubernetes Container Clusters plug-in to service providers. See Publish or Unpublish a Plug-in from a VMware Cloud Director Organization. If you want to enable tenants to create Kubernetes clusters, you must publish the Kubernetes Container Clusters plug-in to those organizations. For more information about managing VMware Cloud Director plug-ins, see Managing VMware Cloud Director Plug-Ins.

7 If you want to grant tenants the rights to create and manage Tanzu Kubernetes clusters, you must publish the **vmware:tkgcluster Entitlement** rights bundle to any organizations that you want to work with clusters. After sharing the rights bundle, you must add the **Edit: Tanzu Kubernetes Guest Cluster** right to the roles you want to create and modify Tanzu Kubernetes clusters. If you want the users also to delete clusters, you must add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the roles. In addition, you can assign the administrator rights to users that you want to view all Tanzu Kubernetes clusters in an organization or users that you want to manage clusters across sites. For information about the rights and access levels for Runtime Defined Entities (RDEs), see Chapter 14 Managing Defined Entities in VMware Cloud Director.

8 Grant access to tenants or system administrators by creating Access Control List (ACL) entries. For more information on sharing Runtime Defined Entities (RDEs), see Sharing Defined Entities in VMware Cloud Director.

9 Create a Tanzu Kubernetes Cluster in the VMware Cloud Director Service Provider Admin Portal

Creating a vSphere with Tanzu Cluster in Your VMware Cloud Director

In VMware Cloud Director, you can use provider VDC and organization VDC Kubernetes policies to create vSphere with Tanzu clusters.

vSphere with Tanzu in VMware Cloud Director

When enabled on a vSphere cluster, vSphere with Tanzu provides the capability to run Kubernetes workloads directly on ESXi hosts and to create upstream Kubernetes clusters in dedicated resource pools. For more information, see the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation.

You can use vSphere with Tanzu in VMware Cloud Director to create provider virtual data centers (VDCs) backed by Supervisor Clusters. A host cluster with enabled vSphere with Tanzu is called a Supervisor Cluster. You can set restrictions on the uses of the resources and limit the available resources, including number of Kubernetes clusters per organization, user, or group. For more information, see Manage Quotas on the Resource Consumption of an Organization in VMware Cloud Director.

To use vSphere with Tanzu in VMware Cloud Director, first, you must enable the vSphere with Tanzu functionality on a vSphere 7.0 or later cluster, and configure that cluster as a Supervisor Cluster. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation. The vCenter Server instance that you want to use can have both host clusters and Supervisor Clusters.

Tenants can create Tanzu Kubernetes clusters by applying one of the organization VDC Kubernetes policies. System administrators can edit and delete organization VDC Kubernetes policies by using the Service Provider Admin Portal or the VMware Cloud Director Tenant Portal. Native and TKGI clusters do not use the provider and organization VDC Kubernetes policies.

VMware Cloud Director provisions Tanzu Kubernetes clusters with the PodSecurityPolicy Admission Controller enabled. You must create a pod security policy to deploy workloads. For information about implementing the use of pod security policies in Kubernetes, see the *Using Pod Security Policies with Tanzu Kubernetes Clusters* topic in the *vSphere with Kubernetes Configuration and Management* guide.

Workflow

1 Add a vCenter Server 7.0 or later instance with an enabled vSphere with Tanzu functionality to VMware Cloud Director. See Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director.

2 Create a provider VDC backed by a Supervisor Cluster. See Create a Provider Virtual Data Center in Your VMware Cloud Director.

   Alternatively, you can add a Supervisor Cluster to an existing provider VDC. If you have a vSphere 6.7 or earlier environment, you can also upgrade the environment to version 7.0 and enable vSphere with Tanzu on an existing cluster.

   Provider VDCs backed by a Supervisor Cluster appear with a Kubernetes icon next to their name in the grid that lists all provider VDCs.

3 (Optional) VMware Cloud Director generates automatically a default provider VDC Kubernetes policy for provider VDCs backed by a Supervisor Cluster. You can create additional provider VDC Kubernetes policies for Tanzu Kubernetes clusters. See Create a Provider VDC Kubernetes Policy in Your VMware Cloud Director.

4 Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director from the **Provider VDCs** tab or Add an Organization VDC Kubernetes Policy in VMware Cloud Director from the **Organization VDCs** tab.

5 Publish the Kubernetes Container Clusters plug-in to service providers. See Publish or Unpublish a Plug-in from a VMware Cloud Director Organization. If you want to enable tenants to create Kubernetes clusters, you must publish the Kubernetes Container Clusters plug-in to those organizations. For more information about managing VMware Cloud Director plug-ins, see Managing VMware Cloud Director Plug-Ins.

6 Publish the **vmware:tkgcluster Entitlement** rights bundle to any organizations that you want to work with Tanzu Kubernetes clusters.

7 Add the **Edit: Tanzu Kubernetes Guest Cluster** right to the roles that you want to create Tanzu Kubernetes clusters. If you want the users also to delete clusters, you must add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the roles. In addition, you can assign the administrator rights to users that you want to view all Tanzu Kubernetes clusters in an organization or users that you want to manage clusters across sites. For information about the rights and access levels for Runtime Defined Entities (RDEs), see Chapter 14 Managing Defined Entities in VMware Cloud Director.

8 Grant access to tenants or system administrators by creating Access Control List (ACL) entries. For more information on sharing Runtime Defined Entities (RDEs), see Sharing Defined Entities in VMware Cloud Director.

9 Create a Tanzu Kubernetes Cluster in the VMware Cloud Director Service Provider Admin Portal

Create a Provider VDC Kubernetes Policy in Your VMware Cloud Director

VMware Cloud Director generates automatically a default provider VDC Kubernetes policy for provider VDCs backed by a Supervisor Cluster. You can create additional provider VDC Kubernetes policies for Tanzu Kubernetes clusters.

Provider VDC and organization VDC Kubernetes policies are necessary only if you want to create or to enable the tenants to create Tanzu Kubernetes clusters. Native and TKGI clusters do not use these Kubernetes policies.

Prerequisites

Verify that you have at least one provider VDC backed by a Supervisor Cluster or add a Supervisor Cluster to an existing provider VDC. See Using Kubernetes with Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of a provider VDC.

3 Under Policies, select **Kubernetes**, and click **New**.

The **Create VDC Kubernetes Policy** wizard appears.

4 Enter a name and description for the provider VDC Kubernetes policy and click **Next**.

5 Select a resource pool backed by a Kubernetes capable Supervisor Cluster.

6 Choose whether you want to reserve CPU and memory for the Kubernetes cluster nodes created in this policy.

   There are two editions for each class type: guaranteed and best effort. A guaranteed class edition fully reserves its configured resources, while a best effort edition allows resources to be overcommitted. Depending on your selection, on the next page of the wizard you can select between VM class types of the guaranteed or best effort edition.

   - Select **Yes** for VM class types of the guaranteed edition for full CPU and Memory reservations.
   - Select **No** for VM class types of the best effort edition with no CPU and memory reservations.

7 Select CPU and Memory limits for the Kubernetes clusters created under this policy.

   When you publish the policy to an organization VDC, the selected limits act as maximums for the newly created organization VDC Kubernetes policy.

8 Click **Next**.

9 On the **Machine classes** page of the wizard, select one or more VM class types available for this policy, and click **Next**.

   The selected machine classes are the only class types available to tenants when you publish the policy to an organization VDC.

10 Select one or more storage policies.

11 Review your choices and click **Finish**.

What to do next

Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director

Edit a vSphere Kubernetes Policy in VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to edit the settings of provider VDC Kubernetes policies used for the creation of organization VDC Kubernetes policies and Tanzu Kubernetes clusters.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of a provider VDC.

3 (Optional) Under Policies, select **Kubernetes**, select the policy you want to publish, and click **Edit**.

   The **Edit VDC Kubernetes Policy** wizard appears.

4 (Optional) Edit the name and description for the provider VDC Kubernetes policy and click **Next**.

5 (Optional) Change the CPU and Memory limits for the Kubernetes clusters created under this policy and click **Next**.

   When you publish the policy to an organization VDC, the selected limits act as maximums for the newly created organization VDC Kubernetes policy.

6 (Optional) On the **Machine classes** page of the wizard, add one or more VM class types available for this policy, and click **Next**.

   The selected machine classes are the only class types available to tenants when you publish the policy to an organization VDC.

7 (Optional) Add one or more storage policies.

8 Review your choices and click **Save**.

What to do next

Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director

Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director

To make a provider VDC Kubernetes policy available to tenants, you can use the VMware Cloud Director Service Provider Admin Portal to publish it to a flex organization VDC. When you publish a provider VDC Kubernetes policy, you create an organization VDC Kubernetes policy that tenants can use to create Kubernetes clusters.

When you add or publish a provider VDC Kubernetes policy to an organization VDC, you make the policy available to tenants. The tenants can use the available organization VDC Kubernetes policies to leverage the Kubernetes capacity while creating Kubernetes clusters. A Kubernetes policy encapsulates placement, infrastructure quality, and persistent volume storage classes. Kubernetes policies can have different compute limits.

You can publish multiple provider VDC Kubernetes policies to a single organization VDC. You can publish a single provider VDC Kubernetes policy multiple times to an organization VDC. You can use the organization VDC Kubernetes policies as an indicator of the service quality. For example, you can publish a Gold Kubernetes policy that allows a selection of the guaranteed machine classes and a fast storage class or a Silver Kubernetes policy that allows a selection of the best effort machine classes and a slow storage class.

Prerequisites

- Create a provider VDC backed by a Supervisor Cluster or add a Supervisor Cluster to an existing provider VDC. See Using Kubernetes with Your VMware Cloud Director.
- Verify that you have at least one flex organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.
- Familiarize yourself with the virtual machine class types for Tanzu Kubernetes clusters. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of a provider VDC.
3. Under Policies, select **Kubernetes**, select the policy you want to publish, and click **Publish**.

   The **Publish to Organization VDC** wizard appears.
4. Enter a tenant-visible name and description for the organization VDC Kubernetes policy and click **Next**.
5. Select the flex organization VDC to which you want to publish the policy and click **Next**.
6. Select CPU and Memory limits for the Kubernetes clusters created under this policy.

   The maximum limits depend on the CPU and Memory allocations of the organization VDC. When you publish the policy, the selected limits act as maximums for the tenants.
7. Choose whether you want to reserve CPU and memory for the Kubernetes cluster nodes created in this policy and click **Next**.

   There are two editions for each class type: guaranteed and best effort. A guaranteed class edition fully reserves its configured resources, while a best effort edition allows resources to be overcommitted. Depending on your selection, on the next page of the wizard you can select between VM class types of the guaranteed or best effort edition.

   - Select **Yes** for VM class types of the guaranteed edition for full CPU and Memory reservations.
   - Select **No** for VM class types of the best effort edition with no CPU and memory reservations.
8. On the **Machine classes** page of the wizard, select one or more VM class types available for this policy.

   The selected machine classes are the only class types available to tenants when you publish the policy to an organization VDC.
9. Select one or more storage policies.
10. Review your choices and click **Publish**.

Results

The information about the published policy appears under the Policies section of the flex organization VDC. The published policy creates a Supervisor Namespace on the Supervisor Cluster with the specified resource limits from the policy.

The tenants can start using the Kubernetes policy to create Kubernetes clusters. VMware Cloud Director places each Kubernetes cluster created under this Kubernetes policy in the same Supervisor Namespace. The policy resource limits become resource limits for the Supervisor Namespace. All tenant-created Kubernetes clusters in the Supervisor Namespace compete for the resources within these limits.

Create a Tanzu Kubernetes Cluster in the VMware Cloud Director Service Provider Admin Portal

You can create Tanzu Kubernetes clusters by using the Kubernetes Container Clusters plug-in.

For more information about the different Kubernetes runtime options for the cluster creation, see Using Kubernetes with Your VMware Cloud Director.

You can manage Kubernetes clusters also by using the VMware Cloud Director Container Service Extension CLI. See the VMware Cloud Director Container Service Extension documentation.

VMware Cloud Director provisions Tanzu Kubernetes clusters with the PodSecurityPolicy Admission Controller enabled. You must create a pod security policy to deploy workloads. For information about implementing the use of pod security policies in Kubernetes, see the *Using Pod Security Policies with Tanzu Kubernetes Clusters* topic in the *vSphere with Kubernetes Configuration and Management* guide.

Prerequisites

- Publish the Kubernetes Container Clusters plug-in to any organizations that you want to manage Tanzu Kubernetes clusters.
- Verify that you have at least one organization VDC Kubernetes policy in your organization VDC. To add an organization VDC Kubernetes policy, see Add an Organization VDC Kubernetes Policy in VMware Cloud Director.
- You must publish the **vmware:tkgcluster Entitlement** rights bundle to any organizations that you want to work with clusters. After sharing the rights bundle, you must add the **Edit: Tanzu Kubernetes Guest Cluster** right to the roles you want to create and modify Tanzu Kubernetes clusters. If you want the users also to delete clusters, you must add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the roles. In addition, you can assign the administrator rights to users that you want to view all Tanzu Kubernetes clusters in an organization or users that you want to manage clusters across sites. For information about the rights and access levels for Runtime Defined Entities (RDEs), see Chapter 14 Managing Defined Entities in VMware Cloud Director.
- Grant access to tenants or system administrators by creating Access Control List (ACL) entries. For more information on sharing Runtime Defined Entities (RDEs), see Sharing Defined Entities in VMware Cloud Director.

Procedure

1. From the top navigation bar, select **More > Kubernetes Container Clusters**.
2. (Optional) If the organization VDC is enabled for TKGI cluster creation, on the **Kubernetes Container Clusters** page, select the **vSphere with Tanzu & Native** tab.
3. Click **New**.
4. Select the **vSphere with Tanzu** runtime option and click **Next**.
5. Enter a name for the new Kubernetes cluster and click **Next**.

6 Select the organization VDC to which you want to deploy a Tanzu Kubernetes cluster and click **Next**.

7 Select an organization VDC Kubernetes policy and a Kubernetes version, and click **Next**.

VMware Cloud Director displays a default set of Kubernetes versions that are not tied to any organization VDC or Kubernetes policy. These versions are a global setting. To change the list of available versions, use the cell management tool to run the `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v` *`version_numbers`* command with comma-separated version numbers.

8 Select the number of control plane and worker nodes in the new cluster.

9 Select machine classes for the control plane and worker nodes, and click **Next**.

10 Select a Kubernetes policy storage class for the control plane and worker nodes, and click **Next**.

11 (Optional) Specify a range of IP addresses for Kubernetes services and a range for Kubernetes pods, and click **Next**.

Classless Inter-Domain Routing (CIDR) is a method for IP routing and IP address allocation.

Option	Description
`Pods CIDR`	Specifies a range of IP addresses to use for Kubernetes pods. The default value is 192.168.0.0/16. The pods subnet size must be equal to or larger than /24. This value must not overlap with the Supervisor Cluster settings. You can enter one IP range.
`Services CIDR`	Specifies a range of IP addresses to use for Kubernetes services. The default value is 10.96.0.0/12. This value must not overlap with the Supervisor Cluster settings. You can enter one IP range.

12 Review the cluster settings and click **Finish**.

What to do next

- Resize the Kubernetes cluster if you want to change the number of worker nodes.
- Download the kubeconfig file. The kubectl command-line tool uses kubeconfig files to obtain information about clusters, users, namespaces, and authentication mechanisms.
- Delete a Kubernetes cluster.

Upgrade a Tanzu Kubernetes Grid Service Cluster in Your VMware Cloud Director Service Provider Admin Portal

You can upgrade Tanzu Kubernetes Grid Service clusters by using the Kubernetes Container Clusters plug-in.

For more information about the VMware Cloud Director Container Service Extension, see the VMware Cloud Director Container Service Extension Documentation.

For Tanzu Kubernetes Grid Service clusters, if the parent supervisor cluster supports a later Kubernetes version, you can upgrade a Tanzu Kubernetes Grid Service cluster in VMware Cloud Director by using the Kubernetes Container Clusters plug-in.

Procedure

1. From the top navigation bar, select **More > Kubernetes Container Clusters**.
2. Click the radio button next to a Tanzu Kubernetes Grid Service cluster you want to upgrade.

   The upgrade column refreshes with information about the availability of an upgrade for the cluster. You can upgrade clusters with status `Available`.
3. Select the Kubernetes version to which you want to upgrade the cluster.
4. Click **Upgrade**.

Managing the VM Storage Policies on a Provider Virtual Data Center in Your VMware Cloud Director

In VMware Cloud Director, you can add, activate, deactivate, and remove VM storage policies from a provider virtual data center (VDC). You can also add, edit, and delete metadata for a VM storage policy on a provider virtual data center.

Starting with VMware Cloud Director 10.2.2, you can limit the allowed entities on a storage policy. See Edit the Entity Types That a VMware Cloud Director Storage Policy Supports .

You can view the list of the storage containers associated with a storage policy by navigating to the **Infrastructure Resources** tab, in the left panel, selecting **Storage Policies**, and clicking the name of the storage policy you want to view.

Sharing Remote Datastores with HCI Mesh

HCI Mesh allows you to expand a vSAN cluster by mounting a remote datastore to the vSAN cluster, which is then mounted to all hosts in the cluster. This results in efficient use and consumption of data center resources, while providing simple storage management at scale. For more information about remote datastores, see the *Administering VMware vSAN* documentation.

Enabling VM Encryption on Storage Policies of a Provider Virtual Data Center in Your VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to add an encryption-enabled storage policy to a provider VDC. You can encrypt VMs and disks by associating a VM or disk with a storage policy that has the VM Encryption capability.

Starting with VMware Cloud Director 10.1, you can improve the security of your data by using VM encryption. Encryption protects not only your virtual machine but also virtual machine disks and other files. You can view the capabilities of storage policies and the encryption status of VMs and disks in the API and UI. You can perform all operations on encrypted VMs and disks that are supported in the respective vCenter Server version.

Enabling VM Encryption

To encrypt VMs in VMware Cloud Director, you must configure at least one Key Management Server (KMS) on your vCenter Server instance and associate the VMs and disks with a storage policy that has the VM Encryption capability.

1. In vCenter Server, add a KMS cluster. A vCenter Server instance can have multiple KMS clusters. For information about setting up a Key Management Server cluster, see the Set up the Key Management Server Cluster topic in the *vSphere Security Guide*.
2. In vCenter Server, enable encryption on a storage policy. See the Create an Encryption Storage Policy topic in the *vSphere Security Guide*.
3. In the VMware Cloud Director Service Provider Admin Portal, add the encryption-enabled policy to a provider VDC. See Add a VM Storage Policy to a Provider Virtual Data Center in Your VMware Cloud Director.
4. In the VMware Cloud Director Service Provider Admin Portal, add the encryption-enabled policy to an organization VDC. See Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center.
5. In the VMware Cloud Director Tenant Portal, tenants can associate the VM or disk with a storage policy with enabled VM Encryption.
6. To decrypt a VM or disk, tenants can associate that VM or disk with a storage policy that does not have encryption enabled.

VM Encryption Limitations

The following actions are not supported in VMware Cloud Director.

- Encrypt or decrypt a powered-on VM or its disks.
- Export an OVF of an encrypted VM.
- Encrypt and decrypt the disks of a VM with a snapshot if the disks are part of the snapshot.
- Decrypt a VM when its disk is on an encrypted policy.
- Add an encrypted disk to a non-encrypted VM.
- Encrypt an existing disk on a non-encrypted VM.
- Add an encrypted named disk to unencrypted VM.
- Create an encrypted linked clone.
- Encrypt a linked clone VM or its disks.
- Instantiate, move, or clone VMs across vCenter Server instances when the source VM is encrypted.

Note On a fast-provisioned organization VDC, if the source or target VM is encrypted and you want to create a clone, VMware Cloud Director always creates a full clone.

Identifying a VM Encryption Storage Capability

By default, **System administrators** and **Organization administrators** have the necessary rights to view the organization VDC storage capabilities and whether VMs and disks are encrypted. **vApp Authors** can view the encryption status of VMs and disks. For more information about roles and rights, see Predefined VMware Cloud Director Roles and Their Rights.

You can view all storage capabilities in the **Capabilities** column under **Resources > vSphere Resources > Storage Policies**. This column displays the VM encryption, tag-based association, vSAN, and IOPS limiting storage capabilities. To view the full list of storage capabilities, expand the row by clicking the arrow on the left side of the storage policy name.

You can also view the storage capability information in the **Storage Policies** tab of a provider VDC.

Add a VM Storage Policy to a Provider Virtual Data Center in Your VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to add a VM storage policy to a provider virtual data center, after which you can configure organization virtual data centers backed by this provider virtual data center to support the added storage policy.

Prerequisites

- Your vSphere administrator created the target VM storage policy. For information about Storage Policy Based Management (SPBM), see the *vSphere Storage* documentation.
- Refresh the Storage Policies of a vCenter Server Instance in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Under **Policies**, select **Storage** and click **Add**.

4 Select one or more storage policies that you want to add, and click **Add**.

   If you select * **(Any)**, VMware Cloud Director dynamically adds and removes datastores as they are added to or removed from the datastore clusters of the provider virtual data center.

What to do next

Configure organization virtual data centers backed by the provider virtual data center to support the storage policy. See Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center.

Activate or Deactivate a VM Storage Policy on a Provider Virtual Data Center in Your VMware Cloud Director

By using the VMware Cloud Director Service Provider Admin Portal, after you deactivate a VM storage policy in a provider virtual data center, its organization virtual data centers cannot use this VM storage policy anymore.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Under **Policies**, select **Storage** .
4. Click the radio button next to the target VM storage policy, and click **Enable** or **Disable**.
5. To confirm, click **OK**.

Delete a VM Storage Policy from a Provider Virtual Data Center in Your VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to delete a VM storage policy from a provider virtual data center.

Prerequisites

Deactivate the target VM storage policy. See Activate or Deactivate a VM Storage Policy on a Provider Virtual Data Center in Your VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Under **Policies**, select **Storage** .
4. Click the radio button next to the target VM storage policy, and click **Remove**.
5. To confirm, click **Remove**.

Modify the Metadata for a VM Storage Policy on a Provider Virtual Data Center in Your VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to add, edit, and delete metadata for a storage policy on a provider virtual data center.

By using object metadata, you can associate user-defined *name=value* pairs with a storage policy on a provider virtual data center. You can use object metadata in vCloud API query filter expressions.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the target VM storage policy, and click **Metadata**.

5 Click **Edit**.

6 (Optional) To add a key-value pair, click **Add**, enter a name and a value, and select a type for the new key-value pair.

7 (Optional) To edit a key-value pair, enter a new name and a value, and select a new type for the key-value pair.

8 (Optional) To remove a key-value pair, in the right end of the row, click the **Delete** icon.

9 Click **Save**, and click **OK**.

Enabling the I/O Operations Per Second Setting in Your VMware Cloud Director

You can use the VMware Cloud Director Service Provider Admin Portal to enable the I/O operations per second (IOPS) setting for a storage policy so that tenants can set per-disk IOPS limits.

Managed read/write performance in physical storage devices and virtual disks is defined in units called IOPS, which measure the read/write operations per second. To limit I/O performance, a provider VDC storage policy that includes storage devices with enabled IOPS allocation must back an organization VDC storage policy. Afterwards, a tenant can configure disks that use it to request a specified level of I/O performance. A storage profile configured with IOPS support delivers its default IOPS value to all disks that use it. That includes disks that are not configured to request a specific IOPS value. A hard disk configured to request a specific IOPS value cannot use a storage policy whose maximum IOPS value is lower than the requested value, or a storage policy that is not configured with IOPS support.

Note The actual I/O throughput that the virtual machines see is a combination of block size and IOPS. If the VMs are using different block sizes, their throughput will be different, even if IOPS is limited to the same number. For more information on managing storage I/O resources, see the *vSphere Resource Management* guide.

Starting with VMware Cloud Director 10.4, to show or hide the IOPS reservations and limits in certain organizations or from certain roles, you can use the **View Disk IOPS** right visible under **Compute > Organization VDC**. The API name of the right is **Organization vDC Disk: View IOPS**.

VMware Cloud Director IOPS Storage Policy

With this option, there are default IOPS settings that you can edit. You can set limits on IOPS per disk or IOPS per storage policy. You can set IOPS limits per disk based on the disk size in GB so that you grant larger disks more IOPS. Tenants can set custom IOPS on a disk within these limits. You can use IOPS limiting with or without IOPS capacity considerations for placement.

1 If you want VMware Cloud Director to consider IOPS when placing disks on datastores, in vCenter Server, add IOPS capacities to all datastores associated with the storage policy you want to modify.

    a In vCenter Server, navigate to **Datastore > customAttribute > Edit**

    b Enter `iopsCapacity, value` as a key-value pair.

    c Click **Add**, and click **Save**.

2 If you want VMware Cloud Director to consider IOPS when placing disks on datastores, in vCenter Server, create a storage policy that uses the datastores with added IOPS capacities.

3 By using the VMware Cloud Director Service Provider Admin Portal or the VMware Cloud Director API, add the storage policy to one or more provider VDCs.

4 By using the Service Provider Admin Portal or the VMware Cloud Director API, publish the storage policy to one or more organization VDCs. The organization VDCs to which you publish the storage policy inherit the policy's IOPS settings.

5 If you want to edit the inherited storage policy IOPS settings, use the Service Provider Admin Portal or VMware Cloud Director API to update the organization VDC storage policy.

This policy type appears as a `VCD/IOPS` capability of the storage policy.

You cannot enable the IOPS limiting on a storage policy backed by a Storage DRS cluster. If you deactivate the VMware Cloud Director **Impact Placement** option from the storage policy settings, you can use a Storage DRS cluster with a `VCD/IOPS` policy. When the **Impact Placement** option is deactivated, vCenter Server and the Storage DRS determine the target datastore as per their IOPS settings. In other words, in this case, you can create or migrate VMs with pre-set IOPS values to Storage DRS clusters, however, Storage DRS validates the IOPS limiting.

vCenter Server IOPS Storage Policy

This option has one IOPS setting for all disks using this policy. You cannot edit this setting in VMware Cloud Director. Tenants cannot set custom IOPS on disks using these policies. This option does not provide IOPS scaling depending on the sizes of the disks or load balancing across datastores.

1 In vCenter Server, create a VC-IOPS enabled storage policy with custom reservation, limit, and shares.

2 In vCenter Server or the VMware Cloud Director Service Provider Admin Portal, assign the disk to the storage policy.

This policy type appears as a `vSphere/IOPS` capability of the storage policy. When the source or target VM has the `vSphere/IOPS` capability, you cannot create fast-provisioned VMs.

Setting IOPS on a Disk in vCenter Server

To change the IOPS setting, in vCenter Server, manually update the IOPS on the disk. You cannot edit these IOPS settings in VMware Cloud Director.

Enabling IOPS Limiting on an Existing Storage Policy

Note You cannot enable VMware Cloud Director IOPS limiting on a policy that already has the `vSphere/IOPS` capability on it.

- Enable IOPS limiting on a `VCD/IOPS` storage policy:

  a If you want VMware Cloud Director to consider IOPS capacities when placing disks on datastores, in vCenter Server, add IOPS capacities to all datastores associated with the storage policy you want to modify.

     1 In vCenter Server, navigate to **Datastore > customAttribute > Edit**

     2 Enter `iopsCapacity, value` as a key-value pair.

     3 Click **Add**, and click **Save**.

  b If you want VMware Cloud Director to consider IOPS capacities when placing disks on datastores, by using the VMware Cloud Director Service Provider Admin Portal or the VMware Cloud Director API, ensure that the corresponding provider VDC storage policy reports the IOPS capacity as non-zero.

  c By using the VMware Cloud Director Service Provider Admin Portal or VMware Cloud Director API, update the organization VDC storage policy to enable the `VCD/IOPS` capability and to set the maximum IOPS value, default IOPS value, and so on.

- Enable the IOPS limiting on a `vSphere/IOPS` storage policy in vCenter Server.

When you enable IOPS limiting for an organization VDC storage policy, tenants can use the VMware Cloud Director Tenant Portal to set per-disk IOPS limits.

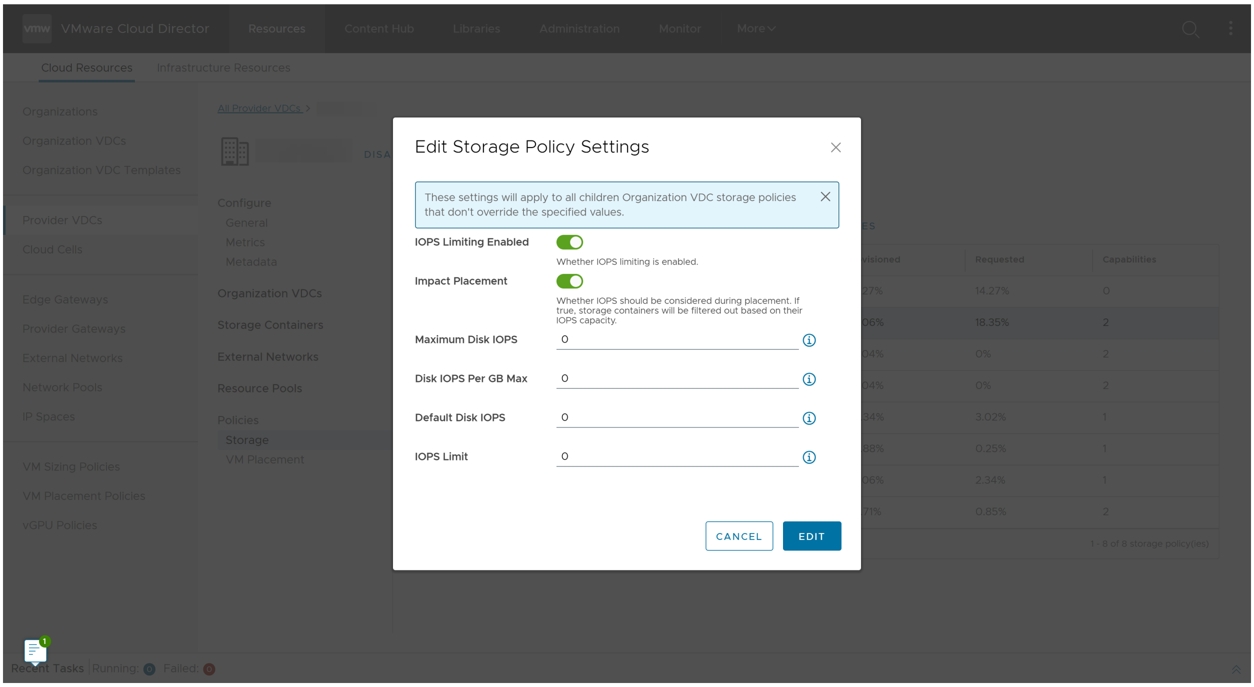
Edit Your VMware Cloud Director Provider VDC Storage Policy Settings

In the Service Provider Admin Portal, you can change the I/O operations per second (IOPS) settings of your provider VDC storage policy. By default, the organization VDCs to which the policy is published inherit the provider VDC storage policy settings.

VMware Cloud Director applies the settings on placement. When you create a new disk or edit an existing one, VMware Cloud Director calculates the IOPS according to the configurations and sets the calculated IOPS for the disk.

If one or more VMs are associated with a storage policy and you change the policy IOPS settings, the VMs and disks continue to have the same values. Only new VMs and new modify operations on existing VMs apply the new IOPS settings to the calculations.

The `Maximum Disk IOPS` and `Disk IOPS Per GB Max` limits are not applicable to **system administrators**.



Edit Storage Policy Settings

These settings will apply to all children Organization VDC storage policies that don't override the specified values.

IOPS Limiting Enabled — Whether IOPS limiting is enabled.

Impact Placement — Whether IOPS should be considered during placement. If true, storage containers will be filtered out based on their IOPS capacity.

Maximum Disk IOPS: 0

Disk IOPS Per GB Max: 0

Default Disk IOPS: 0

IOPS Limit: 0

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the target storage policy, and click **Edit Settings**.

5 If you want to limit the IOPS, turn on the **IOPS Limiting Enabled** toggle.

6 If you want IOPS to be considered during placement, turn on the **Impact Placement** toggle.

   If the **Impact Placement** toggle is turned on, VMware Cloud Director provides IOPS load balancing across datastores. When you set IOPS settings for a disk, VMware Cloud Director considers datastores with enough IOPS capacity for the selected disk. If the **Impact Placement** toggle is turned off, you do not need to set IOPS capacities per datastore and you can use Storage DRS clusters.

7 Configure the maximum and default IOPS settings and click **Save**.

Option	Description
`Maximum Disk IOPS`	The maximum I/O operations per second (IOPS) for all disks associated with this storage policy. The `Default Disk IOPS` and the value calculated by `Disk IOPS Per GB Max` cannot exceed the `Maximum Disk IOPS`.
`Disk IOPS Per GB Max`	The maximum IOPS that can be assigned to any disk associated with this storage policy based on the size of the disk (in GB). This value is also the default IOPS value that VMware Cloud Director uses for any disk associated with this policy. If the value is zero, VMware Cloud Director uses the `Default Disk IOPS` as the default IOPS for the disks associated with this storage policy.
`Default Disk IOPS`	The default IOPS to apply to any disk associated with the storage policy. VMware Cloud Director uses this default only when the `Disk IOPS Per GB Max` value is zero.
`IOPS Limit`	The sum of IOPS across all disks associated with this policy cannot be greater than this value. The `IOPS Limit` is per storage policy.

Results

The new storage policy settings apply to all organization VDCs to which this policy is published.

Edit the Entity Types That a VMware Cloud Director Storage Policy Supports

Starting with VMware Cloud Director 10.2.2, if you do not want a provider VDC storage policy to support certain types of VMware Cloud Director entities, you can edit and limit the list of entities associated with the policy.

When you create a provider VDC storage policy, by default, it supports all available entity types. The default entity types are:

- Virtual machines
- Named disks
- Catalog media
- vApp and VM templates
- Tanzu Kubernetes clusters
- Edge gateways

You can limit the entity types that a storage policy supports to one or more types from this list. When you create an entity, only the storage policies that support its type are available. For example, if you want to create a catalog, the only storage policies that appear are the ones that support catalog media, vApp templates, or both. If an entity uses a storage policy and you remove the type of entity from the list of supported entity types, the entity continues to use the storage policy but you cannot make any changes to it without selecting a new storage policy.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the target storage policy, and click **Edit Supported Types**.

5 From the **Supports Entity Types** drop-down menu, select **Select Specific Entities**.

6 Select the entities that you want the storage policy to support, and click **Save**.

What to do next

- Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center
- Users with the **Supported Storage Entity Type: Manage** right can use the VMware Cloud Director OpenAPI to add or remove entity types from the list of available types for all storage policies. For example, you can add or remove Runtime Defined Entities (RDEs) to the list. For more information about creating extensions that provide additional VMware Cloud Director capabilities to the tenants, see Chapter 14 Managing Defined Entities in VMware Cloud Director.

  VMware Cloud Director automatically applies the changes to the storage policies that support all entities. You cannot remove entities that are selected specifically in one or more storage policies.

Managing the Resource Pools on a VMware Cloud Director Provider Virtual Data Center

In VMware Cloud Director Service Provider Admin Portal, you can add, activate, deactivate, and detach secondary resource pools from a provider virtual data center. You cannot deactivate or detach the primary resource pool on a provider virtual data center.

About the VMware Cloud Director Workload Placement Engine

The VMware Cloud Director placement engine determines on which resources, including resource pools, datastores, and networks or network pools, to place the virtual machines (VMs) in a vApp. Based on each VM requirements, the engine makes the placement decision independently for each VM in a vApp.

The placement engine runs in the following scenarios.

Note VMware Cloud Director places the VMs inside a vApp independently based on the requirements for each VM.

- When you create a VM, the placement engine determines on which resource pool, datastore, and network pool to place it.
- When you start a VM, if the VM fails to power on, VMware Cloud Director can selectively move the VM to another resource pool, datastore, or network pool.
- When you edit a VM changing its datastore, resource, or network configurations, VMware Cloud Director might move the VM to a different datastore and resource pool that support the new VM settings. VMware Cloud Director moves a VM only when the current resources cannot support the new requirements.
- When you migrate VMs to different resource pools.
- When an organization virtual data center (VDC) discovers VMs created in any vCenter Server resource pool that backs the VDC, and the system constructs a simplified vApp to contain each discovered VM.

The placement engine uses the following criteria to select candidate resource pools for a VM.

- CPU capacity
- Memory capacity
- Number of virtual CPUs
- Hardware version supported by the host and allowed by the provider VDC
- Affinity rules

The placement engine filters out deactivated resource pools from the candidate list. When possible, VMware Cloud Director places VMs on the same host cluster as other VMs in the organization VDC.

Important VM-Host affinity rules must have a condition that the rule `must run` on hosts in group. VM-Host anti-affinity rules must have a condition that the rule `must not run` on hosts in group.

The placement engine uses the following criteria to select candidate datastores for VMs.

- Storage capacity and thresholds
- Storage policies
- Affinity requirements between VMs
- If IOPS is activated, IOPS capacity and VM disks IOPS

There are two datastore thresholds in VMware Cloud Director.

- Red threshold - the amount of free space on a datastore, below which, VMware Cloud Director filters out the datastore during the placement of any entity such as a VM, a template, or a disk.

  When a datastore reaches its red threshold, the workload placement engine stops placing new VMs on the datastore except while importing VMs from vCenter Server. In the case of VM import, if the vCenter Server VM is already present on the red threshold datastore, the placement engine prefers the existing datastore.

  The workload placement engine uses the red threshold for all workflows. When making a request for any new placement, the placement engine first filters out any datastores or storage pods which have breached the red threshold. When making a placement request for an existing entity, if the disks are residing on the datastores that are breaching the red threshold, VMware Cloud Director relocates the disks to other available datastores. Then, the engine selects a datastore out of the remaining datastores or storage pods, either through the selector logic of VMware Cloud Director or from the vSphere Storage DRS recommendations.

- Yellow threshold - the amount of free space on the datastore, below which VMware Cloud Director filters out the datastore during the placement of shadow VMs from which VMware Cloud Director creates fast-provisioned VMs. For more information on shadow VMs, see Fast Provisioning of Virtual Machines.

  The yellow threshold does not apply to the linked clones that VMware Cloud Director uses for fast provisioning of VMs. When the placement engine selects a datastore for a linked clone, if the selected datastore is missing a shadow VM, VMware Cloud Director creates a shadow VM on the datastore. The threshold does not apply to the shadow VM in this case.

  The yellow threshold applies only to the periodic background job creating shadow VMs. If activated, the job runs every 24 hours and uses eager VM creation on each datastore for a given hub and storage policy pair. To activate the job for eager provisioning of shadow VMs, you must set the following property to `true`.

  ```
  valc.catalog.fastProvisioning=true
  ```

  Note The periodic background job creates shadow VMs on all datastores for all templates. The job increases the storage consumption even when you are not using the datastores or shadow VMs.

In most cases, the placement engine filters out deactivated and red threshold datastores from the candidate list. The engine does not filter out these datastores when you import a VM from vCenter Server.

When implementing the threshold logic, VMware Cloud Director does not evaluate the requirements of the current placement subject. For the workload placement engine to place a subject on a datastore, the available space in bytes must be more than the threshold in bytes. For example, for a datastore with available capacity of 5 GB with a red threshold set at 4 GB, the placement engine can place a VM with a requirement for 2 GB. If the VM creation breaches the threshold, the placement engine filters out the datastore for further placements.

The placement engine uses the network name to select candidate network pools for a vApp and its VMs.

After the placement engine selects a set of candidate resources, it ranks the resources and picks the best location for each VM based on the CPU, virtual RAM, and storage configuration of each VM.

While ranking resources, the placement engine examines the current and estimated future resource use. Estimated future use is calculated based on powered-off VMs currently placed on a given resource pool and their expected use after they are powered on. For CPU and memory, the placement engine considers the current unreserved capacity, the maximum use, and the estimated future unreserved capacity. For storage, the engine considers the aggregate provisioned capacity provided by the cluster that each resource pool belongs to. The placement engine then considers the weighted metrics of the current and future suitability of each resource pool.

When a move is necessary, the placement engine favors resource pools with the most unreserved capacity for CPU, memory, and storage. It also gives lower preference to yellow clusters so that yellow clusters are only selected if no healthy cluster is available that satisfies the placement criteria. When importing a VM from vCenter Server, if the VM placement is satisfactory, to minimize movement, the engine ignores the thresholds.

When you power on a VM, VMware Cloud Director tries to power it on in its current location. If vCenter Server reports an error with the host CPU and memory capacity, VMware Cloud Director tries the resource pool twice before trying to move the VM to the other compatible resource pools on the organization VDC. While rerunning the placement engine to attempt to find a compatible resource pool, VMware Cloud Director excludes previous tried and failed resource pools. If no suitable resource pools are connected to the datastore the VMDKs are located on, moving a VM to another resource pool can cause the migration of the VM's VMDKs to a different datastore. If the VM placement fails in all locations that satisfy the requirements of the VM, VMware Cloud Director returns an error message that the placement is not feasible. If there is an affinity to the current datastore and the datastore is unavailable, the placement engine returns an error that the placement is not feasible. This is a normal state of the system when it operates near full capacity and the proposed solution does not meet all the requirements at the current time. To remediate the error, you can add or free up resources and initiate a retry. When there is no specific datastore required, the placement engine selects a datastore in the candidate host cluster or resource pool that fulfills the other requirements such as storage policy, storage capacity, and IOPS capacity.

During concurrent deployment situations when a resource pool is close to capacity, the validation of that resource pool might succeed even though the resource pool lacks the resources to support the VM. In these cases, the VM cannot power on. If a VM fails to power on in this situation and there is more than one resource pool backing the VDC, to prompt VMware Cloud Director to migrate the VM to a different resource pool, start the power on operation again.

When the cluster that a resource pool belongs to is close to capacity, a VM on that resource pool might not be able to power-on if no individual host has the capacity to power on the VM. This happens as a result of capacity fragmentation at the cluster level. In such cases, a system administrator must migrate a few VMs out of the cluster so that the cluster maintains sufficient available capacity.

VM Placement Engine Algorithm

The placement algorithm picks a host cluster from the list of host clusters that have required storage profiles available and satisfy any existing VM-VM, VM-host affinity, or anti-affinity rules. VMware Cloud Director calculates the placement solution through various scores. To change the behavior of the engine, you can use the cell management tool to modify the configurable parameters that begin with the underscore (_) symbol.

1 For each host cluster the workload placement engine calculates a `capacityScore`, `futureCapacityScore`, and `reservationScore`. The placement engine calculates each score separately for CPU, memory, and storage.

```
capacityScore: (not available in some cases )

CPU = (cpuUnreservedCapacityMHz - (cupBurstMHz * _cpuBurstRatio)) / cpuRequirementMHz
Memory = (memoryUnreservedCapacityMB - (memBurstMB * _memoryBurstRatio)) /
memRequirementMB
Storage = storageFreeCapacityMB / stgRequirementMB

futureCapacityScore (not available in some cases)

CPU = (cpuUnreservedCapacityMHz - (cpuUndeployedReservationMHz * _futureDeployRatio)) /
cpuRequirementMHz
Memory = (memoryUnreservedCapacityMB - (memUndeployedReservationMB *
_futureDeployRatio)) / memRequirementMB
Storage = storageFreeCapacityMB / stgRequirementMB

reservationScore: (used for capacityScore and futureCapacityScore when those scores are
unavailable)

CPU = cpuUnreservedCapacityMHz / cpuRequirementMHz
Memory = memoryUnreservedCapacityMB / memRequirementMB
Storage = storageFreeCapacityMB / stgRequirementMB
```

2 For each host cluster, the placement engine calculates a `weightedCapacityScore` for CPU, memory, and storage.

```
weightedCapacityScore = capacityScore * _currentScoreWeight + futureCapacityScore * (1 -
_currentScoreWeight)
```

Each weightedCapacityScore is a ratio from 0 through 1 with higher values representing more available resources. weightedCapacityScore values can be compared across different resource types, for example, CPU, memory, and storage, because they represent a unit-less measure of availability. Higher weightedCapacityScore means more availability of the corresponding resource in the host cluster.

3 The placement engine verifies that there are enough resources for CPU, memory, and storage.

```
totalAvailable * _[memory|cpu|storage]headRoom < free / UnreservedCapacity
```

4 The placement engine sorts the list of host clusters on the weightedCapacityScore so that the least constrained host cluster is first and the most constrained host cluster is last.

5 The placement engine processes each host cluster in the list.

- If the host cluster must be avoided, for example, because of anti-affinity rule, the engine adds it to avoidHubList.
- If the host cluster does not have enough additional resources, the engine adds it to noHeadRoomHubList.
- If the host cluster is preferred, for example, because of a strong affinity rule or the current host cluster, the engine adds it to preferredHubList.
- All other host clusters go to acceptableHubList.

Within each list, the most preferred host cluster is first and the least preferred host cluster is last.

6 The engine integrates the four lists.

```
preferredHubList + acceptableHubList + noHeadRoomHubList + avoidHubList
```

The engine orders the resulting list from the most preferable to the least preferable host cluster.

7 The placement engine picks the top host cluster from the list as the target hub.

Adjustable Parameters

To influence various selection algorithm thresholds, there are several parameters that you can customize. However, only service provider administrators with advanced knowledge of the VMware Cloud Director operations might attempt changing these parameters from their default values because it might produce undesirable and unexpected results. Test any parameter changes in a non-production environment first.

You can customize the following parameters by using the Cell Management Tool.

Parameter	Description
`vcloud.placement.ranking.currentScoreWeight`	The relative importance of the current component of the host cluster score. The value must be in [0.1]. When the value is 0, the engine ranks the host cluster only based on future score. When the value is 1, the engine ranks the host cluster only based on the current score. The default is 0.5.
`vcloud.placement.ranking.memoryBurstRatio` `vcloud.placement.ranking.cpuBurstRatio`	The percentage of allocation beyond reservation of a VM that the ranker uses to estimate the load of the cluster. The value is from 0 through 1. 0 means a VM only uses its reservation. 1 means the VM is fully busy. The default is 0.67.
`vcloud.placement.ranking.futureDeployRatio`	The percentage of VMs on this host cluster that are expected to be deployed and to consume memory and CPU. The value is from 0 through 1. The default is 0.5.

`vcloud.placement.ranking.memoryHeadRoom`
`vcloud.placement.ranking.cpuHeadRoom`
`vcloud.placement.ranking.storageHeadRoom`
	These parameters give the control for leaving additional resources for growth on a host cluster. The engine defines the headroom as a ratio of unreserved resources. For example, if `vcloud.placement.ranking.memoryHeadRoom` is 0.2, after a host cluster has less than 20% resources available, the engine considers it as a cluster with insufficient memory headroom and will rank it lower than other host clusters. The value must be from 0 through 1. The default is 0.2.
	Example:
	`./cell-management-tool manage-config -n vcloud.placement.ranking.memoryHeadRoom -v 0.3`

Datastore Filters and Storage Placement Algorithm

VMware Cloud Director datastore filters and storage placement algorithm determine the placement of VM files and disks on the underlying storage resources.Storage containers represent the storage resources, either datastore or datastore cluster.

The datastore filters are part of the storage filter chain, which helps narrow down the eligible storage containers, based on the requirements of the placement subject. The filters use the available storage containers in a provider VDC as an input list. The filters run in a predefined sequence, and each filter passes the refined list of storage containers to the next filter. VMware Cloud Director skips the inapplicable filters. For example, for VMs without an IOPS setting, VMware Cloud Director does not run the IOPS filter.

Table 6-1. Datastore Filters

Filter	Description
`AffinityDatastoreFilter`	Filters the storage containers based on the affinity and anti-affinity rules defined for the datastores. VMware Cloud Director sets datastore affinity rules in the cases like VM import from vCenter Server, tenant migration, and so on.
`AlreadyOnValidDatastoreFilter`	If a placement subject is already placed on a valid datastore, this filter rejects all other storage containers and retains only the valid datastore.
`BadHostsFilter`	Filters out the storage containers that do not have at least one connected, operational, and powered on host. Filters out storage containers that have been deleted from the inventory.
`DatastoreClusterFilter`	Filters out all datastore clusters and the datastores that are part of a datastore cluster. This filter is used when the placement subject does not require datastore clusters. For example, if shared named disks are not allowed on the datastore clusters, based on `config: vcloud.disk.shared.allowOnSpod`.
`DatastoreFsFilter`	Filters out all storage containers that are part of the specified file system. For example, if shared named disks are not allowed on NFS datastores, based on `config: vcloud.disk.shared.allowOnNfs`, then, the placement algorithm adds this filter to the chain.
`DisabledDatastoreFilter`	Filters out all deactivated storage containers from the input list.
`IopsCapacityDatastoreFilter`	Filters out all datastores that do not have enough IOPS capacity for the VM. The filter runs if the following prerequisites are met. ■ The VM has an IOPS setting. ■ There are no storage pods. ■ All datastores have `iopsCapacities` set. ■ The VM has activated **VCD/IOPS** capability of the storage policy and the **Impact Placement** option from the storage policy settings is activated.
`LeastProvisionedFilter`	Singles out the least provisioned storage container.
`LinkedCloneFilter`	Filters out all the datastores that do not have a source VM or corresponding shadow VMs on a datastore. Filters out any datastores that have source VMs with exceeded allowed maximum chain length for the virtual disks of the VMs.

Table 6-1. Datastore Filters (continued)

Filter	Description
`MinFreeSpaceFilter`	Filters out any storage containers that do not contain enough free space for the placement subject. For storage pods, the maximum free space of the child datastores determines the free space and not the total free space of the child datastores or the free space of the storage pod. For example, if a storage pod has two datastores, respectively, with 3 GB and 5 GB free. VMware Cloud Director considers the free space of the storage pod to be 5 GB. If there are no such containers, the filter keeps the container with most free space.
`MostFreeSpaceFilter`	Singles out the storage container with most free space.
`StorageClassFilter`	Filters out any storage containers or storage pods that do not match the storage policy of the placement subject, defined in their requirement.
`ThresholdFilter`	Filters out the storage containers that reach the specified threshold of available capacity. There are yellow and red thresholds in VMware Cloud Director. See Configure Low Disk Space Thresholds for a Provider Virtual Data Center Storage Container in Your VMware Cloud Director.
`VirtualMachineFilter`	Filters out all storage containers that the specified VM does not have access to.

VMware Cloud Director passes the final list of filtered storage containers to the storage placement algorithm which tries to place the placement subject into the selected storage containers.

To place the set of placement subjects in the best possible datastore for each, the storage placement algorithm uses configurable criteria and the list of valid datastores. The storage placement algorithm uses the following workflow.

1 Receives from the placement engine a set of placement subjects and a target resource pool that backs the provider VDC. There are two alternatives.

   - Usually, the algorithm receives a VM home file containing metadata and configuration information and a set of disks for regular, non-fast-provisioned VM placement.
   - The algorithm might use an aggregate disk approach for named disks and fast provisioned VMs. In other words, for each fast provisioned VM, the algorithm receives one requirement for the VM and all of its disks.

2 Receives the set of storage containers eligible for that hub, which includes both datastores and storage pods.

3 To filter out the storage containers that cannot fit a subject, for each placement subject, the algorithm runs through the static chain of placement filters. For example, if a VM disk cannot fit on a datastore, the algorithm marks the datastore as not eligible for the VM disk.

4. Ranks the storage containers for each subject in order of their preference following consecutively the subsequent considerations.
   a. Whether the container is as storage pod or a datastore
   b. How many other placement subjects contain the storage pod as a valid container
   c. Size of the container
5. If any of the containers is a storage pod, to reduce the storage pods down to datastores, the algorithm runs the vSphere Storage DRS invocation algorithm.
6. After inputting the placement subjects and their set of valid datastores, determines where the placement subject must reside.
7. Returns a final placement result that determines the datastores on which each placement subject must reside, or returns an error that the VMware Cloud Director algorithm cannot find a suitable placement.

Add a Resource Pool to a VMware Cloud Director Provider Virtual Data Center

In VMware Cloud Director Service Provider Admin Portal, you can add one or more secondary resource pools to a provider virtual data center, so that its Pay-As-You-Go and Allocation Pool organization virtual data centers can expand.

When compute resources are backed by multiple resource pools, they can expand to accommodate more virtual machines.

You can add resource pools backed by vSphere clusters that are optimally configured for hosting NSX edges that have VLAN uplinks. VMware Cloud Director can use metadata to indicate that the system must place organization VDC Edge Gateways in resource pools backed by those clusters. For more information, see VMware Knowledge Base Article https://kb.vmware.com/kb/2151398.

Prerequisites

Your vSphere administrator created the target secondary resource pool in the vCenter Server instance that backs the primary resource pool of the provider virtual data center.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. On the **Resource Pools** tab, click **Add**.
4. Select the resource pool you want to add, and click **Add**.

   If you want to use vSphere with Tanzu, select a Supervisor Cluster. VMware Cloud Director displays a Kubernetes icon next to resource pools backed by a Supervisor Cluster.

5 If you select a resource pool or cluster that is backed by a Supervisor Cluster, to establish a trust relationship with the Kubernetes control plane, you must trust the Kubernetes control plane certificate.

6 If you want to add an additional resource pool, repeat Step 1 to Step 5.

Results

VMware Cloud Director adds the resource pool for the provider virtual data center to use, making elastic all Pay-As-You-Go and Allocation Pool organization virtual data centers backed by the provider virtual data center.

VMware Cloud Director also adds a System VDC resource pool beneath the new resource pool. This resource pool is used for the creation of system resources such as NSX edge VMs and VMs that serve as a template for linked clones.

Important Do not edit or delete the System VDC resource pool.

Activate or Deactivate a Resource Pool on a VMware Cloud Director Provider Virtual Data Center

In VMware Cloud Director Service Provider Admin Portal, when you deactivate a resource pool, the memory and compute resources of the resource pool are no longer available to the provider virtual data center.

Processes that are already in progress do not stop using resources from the deactivated resource pool.

Note You cannot deactivate the primary resource pool on a provider virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 Click the **Resource Pools** tab.

4 Click the radio button next to the target resource pool, and click **Enable** or **Disable**.

5 To confirm, click **OK**.

Detach a Resource Pool from a VMware Cloud Director Provider Virtual Data Center

If a provider virtual data center has more than one resource pool, in VMware Cloud Director Service Provider Admin Portal, you can detach a secondary resource pool from the provider virtual data center. You cannot detach the primary resource pool from the provider virtual data center.

Prerequisites

- Deactivate the target resource pool on the provider virtual data center. See Activate or Deactivate a Resource Pool on a VMware Cloud Director Provider Virtual Data Center.
- Redeploy any networks that are affected by the deactivated resource pool.
- Redeploy any edge gateways that are affected by the deactivated resource pool.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Click the **Resource Pools** tab.
4. Click the radio button next to the target resource pool, and click **Detach**.
5. To confirm, click **OK**.

Migrate VMs Between Resource Pools on a VMware Cloud Director Provider Virtual Data Center

In VMware Cloud Director Service Provider Admin Portal, you can migrate VMs from one resource pool to another on the same provider virtual data center. You can migrate virtual machines to populate a recently added resource pool, to depopulate a resource pool you plan to decommission, or to manually balance the resources of the provider virtual data center.

You cannot migrate VMs that are part of a reservation pool organization virtual data center. You must migrate templates and media separately using datastore migration.

Prerequisites

Verify that you have at least one resource pool on the provider virtual data center other than the resource pool the virtual machines are on.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Select **Resource Pools**.
4. Click the name of the resource pool from which you want to migrate VMs.
5. Select one or more VMs that you want to migrate and click **Migrate VM**.

6 Choose between an automatic or manual selection of the destination resource pool for the VM migration.

Option	Description
Automatically select a resource pool	VMware Cloud Director selects the destination resource pool for the VMs based on the current resource balance of all available resource pools.
Manually select a resource pool	Select a resource pool from the list of available resource pools to which to migrate the VM to.

7 (Optional) Select the check box to allow the migration of the selected VMs to a different datastore.

8 Click **Migrate**.

Modify the Metadata for a VMware Cloud Director Provider Virtual Data Center

In VMware Cloud Director Service Provider Admin Portal, you can add, edit, and delete metadata for a provider virtual data center.

By using object metadata, you can associate user-defined *name=value* pairs with a provider virtual data center. You can use object metadata in vCloud API query filter expressions.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.

3 On the **Configure > Metada** tab, in the upper right corner, click **Edit**.

4 (Optional) To add a key-value pair, click **Add**, enter a name and a value, and select a type for the new key-value pair.

5 (Optional) To edit a key-value pair, enter a new name and a value, and select a new type for the key-value pair.

6 (Optional) To remove a key-value pair, in the right end of the row, click the **Delete** icon.

7 Click **Save**, and click **OK**.

Managing VMware Cloud Director Organizations

7

The VMware Cloud Director Service Provider Admin Portal allows you to create, configure, and manage VMware Cloud Director organizations.

Use VMware Cloud Director Service Provider Admin Portal to manage organizations, set policies to determine how users consume resources allocated to an organization, and manage publishing and sharing of catalogs.

Read the following topics next:

Understanding Leases in VMware Cloud Director

Creating a VMware Cloud Director 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 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, VMware Cloud 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, VMware Cloud Director marks the vApp or vApp template as expired, or deletes the vApp or vApp template, depending on the organization policy you set.

Create a VMware Cloud Director Organization

You can create a new organization from the VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources**, and click **Cloud Resources**.

   a. From the left panel, select **Organizations**.

   The list of existing organizations displays in a grid view.

2. Click **New**.

   The **New Organization** dialog opens.

3. Enter the following values.

Option	Description
Organization name	The unique identifier that forms the URL for accessing the Tenant Portal of the organization.
Organization full name	Full name of the organization.
Description	An optional description for the organization.

4. Click the **Create** button to complete the creation.

Activate or Deactivate a VMware Cloud Director Organization

Deactivating a VMware Cloud Director organization prevents users from logging in to the organization and terminates the sessions of users that are currently logged in. Running vApps in the organization continue to run.

As a **system administrator**, you can allocate resources, add networks, and so on, even after you deactivate an organization.

Procedure

1 From the top navigation bar, select **Resources**, and click **Cloud Resources**.

   a From the left panel, select **Organizations**.

   The list of existing organizations displays in a grid view.

2 Click the radio button next to the name of the organization and click **Enable** or **Disable**.

Delete a VMware Cloud Director Organization

Delete an organization to permanently remove it from VMware Cloud Director.

Prerequisites

Before you can delete an organization, you must deactivate it and delete all organization virtual data centers, templates, media files, and vApps in the organization.

Procedure

1 From the top navigation bar, select **Resources**, and click **Cloud Resources**.

   a From the left panel, select **Organizations**.

   The list of existing organizations displays in a grid view.

2 Click the radio button next to the name of the organization and click **Delete**.

3 To confirm, click **Yes**.

Working with External Resources for Application Images in Your VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5, you can use Content Hub for centralized content management of application images.

Application Images

An application image is a catalog item that contains all application specific details, such as application name, application version, application logo, screenshots, and any additional information necessary to consume the application. After upgrading to version 10.5, all pre-existing catalog items, such as vApp templates and media files, appear as application images. You can still see the catalog items as vApp templates, virtual machines within the vApps, and media files.

External Resources for Application Images

With Content Hub, VMware Cloud Director can integrate with multiple external content sources, such as VMware Marketplace and external Helm chart repositories.

Service providers can create multiple catalog content resources for both VMware Marketplace and external Helm chart repositories, while tenants can create catalog content resources only for external Helm chart repositories. Tenants can deploy Helm chart container applications from these catalog content resources to Kubernetes clusters they own or to clusters other tenants share with them.

External Source	Helm Chart Application Image	VM Application Image
VMware Marketplace	✓	✓
Helm chart repository	✓	

Working with VMware Marketplace Resources in Your VMware Cloud Director Service Provider Admin Portal

VMware Marketplace is an online platform that serves as a catalog content resource for the distribution, discovery, and deployment of container applications. Using the VMware Cloud Director Service Provider Admin Portal, you can create a VMware Marketplace resource and deploy Helm chart container applications from these catalog content resources to Kubernetes clusters.

Create a VMware Marketplace Resource in Your VMware Cloud Director Service Provider Admin Portal

If you want tenants to import applications from VMware Marketplace into VMware Cloud Director catalogs, you must create a VMware Marketplace resource and share it with one or more tenant organizations.

A VMware Marketplace resource stores all the information you need to establish a connection with VMware Marketplace, to enable users to browse contents from a remote VMware Marketplace, and to import VMware Marketplace applications.

Prerequisites

- Verify that you have the **Edit the External Source in Content Hub** right.
- Verify that you have the token ID of a valid VMware Marketplace API token. See Generate API Tokens in the *VMware Cloud Services Product Documentation*.

Procedure

1. From the top navigation bar, select **Content Hub**.
2. From the left panel, select **VMware Marketplace**.
3. Click **New**.
4. Enter a name and, optionally, a description of the VMware Marketplace resource.
5. Enter the API URL for the VMware Marketplace production instance.

   The URL must be in the `https://gtw.marketplace.cloud.vmware.com/api/v1` format.

6 Enter the API token ID of a valid VMware Marketplace token.

7 Enter the **VMware Marketplace** resource details.

8 Click **Save**.

   The VMware Marketplace connection appears in the list of resources.

What to do next

To modify the resource, click the vertical ellipsis next to the resource name, and select **Edit**.

Share a VMware Marketplace Resource Using Your VMware Cloud Director Service Provider Admin Portal

As a VMware Cloud Director service provider administrator, you can share the configured VMware Marketplace resources with tenant organizations.

Prerequisites

- Verify that your service provider created a VMware Marketplace resource. For information about the creation of VMware Marketplace resources, see Create a VMware Marketplace Resource in Your VMware Cloud Director Service Provider Admin Portal in the *VMware Cloud Director Service Provider Admin Guide*.
- Verify that you have the **Share the Content Hub External Source** right.

Procedure

1 From the top navigation bar, select **Content Hub**.

2 From the left panel, select **VMware Marketplace**.

3 Click the vertical ellipsis next to the resource name, and select **Share**.

4 Select the tenant organizations with which you want to share the resource, and click **Save**.

   You can set the individual access level for the respective tenant organization only to **Read Only**.

Delete a VMware Marketplace Resource Using Your VMware Cloud Director Service Provider Admin Portal

Using VMware Cloud Director Service Provider Admin Portal, you can delete an existing VMware Marketplace resource.

Prerequisites

- Verify that no templates are imported from the VMware Marketplace resource that you want to delete.
- Verify that you have the **Delete the External Source from Content Hub** right.

Procedure

1 From the top navigation bar, select **Content Hub**.

2 From the left panel, select **VMware Marketplace**.

3 Click the vertical ellipsis next to the resource name, and select **Delete**.

4 Click **Delete**.

Working with External Helm Chart Repository Resources in Your VMware Cloud Director Service Provider Admin Portal

Using the VMware Cloud Director Service Provider Admin Portal, you can deploy specific applications and services on a Kubernetes cluster by using a Helm chart package that contains pre-configured Kubernetes resources, including deployments, services, ingress rules, and other components.

The Helm chart package provides a template that you can use to customize the configuration parameters of the chart during deployment.

Create an External Helm Chart Repository Resource in Your VMware Cloud Director Service Provider Admin Portal

If you want tenants to import applications from an external Helm chart repository into VMware Cloud Director catalogs, you must create a Helm chart repository resource and share it with one or more tenant organizations.

A Helm chart repository resource stores all the information you need to establish a connection with a Helm chart repository, to enable users to browse contents from a remote Helm chart repository, and to import Helm chart repository applications.

You can create one or more Helm chart repository resources in your VMware Cloud Director Service Provider Admin Portal.

Prerequisites

- Verify that you have the **Edit the External Source in Content Hub** right.
- Verify that you have a configured Helm chart repository. To establish a connection between VMware Cloud Director and a Helm chart repository, you need the URL of the repository. If you are adding the repository with a basic authorization, you also need the credentials of the repository user account.
- Verify that the repository contains an `index.yaml` file. For example, if the repository is located at `https://example.com/charts`, the index file must be available at `https://example.com/charts/index.yaml`. If you are connecting to a Harbor server, refer to the Harbor documentation for the available repository URLs. A typical location, for example, is `https://<harbor-server>/chartrepo/<project>`.

Procedure

1 From the top navigation bar, select **Content Hub**.

2 From the left panel, select **Helm Chart Repository**.

3. Click **New**.
4. Enter a name and, optionally, a description of the Helm chart repository resource.
5. Enter the URL for the Helm chart repository resource.
6. Select the authentication type.

   If you are adding the repository with a basic authorization, you must enter the credentials of the repository user account.
7. Click **Save**.

   The Helm chart repository resource appears in the list of configured resources.

What to do next

You can keep VMware Cloud Director up to date with the latest collection of application images from the Helm chart repository by clicking the vertical ellipsis and selecting **Sync**.

To modify the resource, click the vertical ellipsis next to the resource name, and select **Edit**.

Share an External Helm Chart Repository Resource Using Your VMware Cloud Director Service Provider Admin Portal

As a VMware Cloud Director service provider administrator, you can share the configured Helm chart repository resources with other tenant organizations.

Prerequisites

Verify that you have the **Share the Content Hub External Source** right.

Procedure

1. From the top navigation bar, select **Content Hub**.
2. From the left panel, select **Helm Chart Repository**.
3. Click the vertical ellipsis next to the resource name, and select **Share**.
4. Select the tenant organizations with which you want to share the resource, and click **Save**.

   You can set the individual access level for the respective tenant organization only to **Read Only**.

Delete an External Helm Chart Repository Resource Using Your VMware Cloud Director Service Provider Admin Portal

Using VMware Cloud Director Service Provider Admin Portal, you can delete an existing Helm chart repository resource.

Prerequisites

- Verify that no templates are imported from the Helm chart repository resource that you want to delete.
- Verify that you have the **Delete the External Source from Content Hub** right.

Procedure

1. From the top navigation bar, select **Content Hub**.
2. From the left panel, select **Helm Chart Repository**.
3. Click the vertical ellipsis next to the resource name, and select **Delete**.
4. Click **Delete**.

Configure Catalogs for a VMware Cloud Director Organization

In VMware Cloud Director Service Provider Admin Portal, you can configure how an organization shares its service catalogs.

Note Deactivating the **Share catalogs with other organizations** option does not stop the sharing of affected catalogs.

Procedure

1. From the top navigation bar, select **Resources**, and click **Cloud Resources**.

   a. From the left panel, select **Organizations**.

   The list of existing organizations displays in a grid view.
2. Select an organization, and under the **Configure** tab, select **Catalog**.
3. To change the sharing and publishing settings, click **Edit**.

Option	Description
Sharing	Allows organization administrators to share this organization's catalogs with other organizations in this instance of VMware Cloud Director. If you do not select this option, organization administrators are still able to share catalogs within the organization.
Allow publishing to external catalogs	Allows organization administrators to publish catalogs to organizations outside of this instance of VMware Cloud Director.
Allow subscribing to external catalogs	Allows organization administrators to subscribe to catalogs outside of this instance of VMware Cloud Director.

Configure Policies for a VMware Cloud Director Organization

Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. In VMware Cloud Director Service Provider Admin Portal, you can modify these settings to prevent users from depleting or monopolizing an organization's resources.

Prerequisites

See Understanding Leases in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources**, and click **Cloud Resources**.

a From the left panel, select **Organizations**.

The list of existing organizations displays in a grid view.

2 Select an organization and select the **Policies** tab.

3 To edit the leases, quotas, resource limits, and password policies for the organization, click **Edit**.

4 Configure vApp leases with the following settings.

Option	Description
Maximum runtime lease	How long vApps can run before they are automatically stopped.
Runtime expiry action	How expired running vApps are processed. Suspending a vApp, suspends all its virtual machines and preserves their current state by writing the memory to disk. **Power off** immediately stops all its virtual machines and child vApps.
Maximum storage lease	How long stopped vApps are available before being automatically cleaned up.
Storage cleanup	How vApps are processed after being stopped and cleaned up.

5 Configure vApp template leases with the following settings.

Option	Description
Maximum storage lease	How long vApp templates are available before being automatically cleaned up.
Storage cleanup	How expired vApp templates are processed after being cleaned up.

6 Configure quotas with the following settings.

Option	Description
All VMs quota	Total number of available VMs a user can store in this organization.
Running VMs quota	Total number of VMs a user can power on in this organization.

7 Configure limits with the following settings.

Option	Description
Number of resource intensive operations per user	Enter the maximum number of simultaneous resource intensive operations per user, or select **Inherit System Limit**.
Number of resource intensive operations to be queued per user	Enter the maximum number of queued resource intensive operations per user, or select **Inherit System Limit**.
Number of resource intensive operations per organization	Enter the maximum number of simultaneous resource intensive operations per organization, or select **Inherit System Limit**.
Number of resource intensive operations to be queued per organization	Enter the maximum number of queued resource intensive operations per organization, or select **Inherit System Limit**.

Option	Description
Number of simultaneous connections per VM	Enter the maximum number of simultaneous console connections per virtual machine, or select **Inherit System Limit**.
Number of virtual data centers per organization	Enter the maximum number of organization virtual data centers per organization, or select **Inherit System Quota**.

8 Configure password policies with the following settings.

Option	Description
Account lockout enabled	Enable user account lockout after a number of invalid login attempts.
Invalid logins before lockout	Number of invalid login attempts before the user account is locked.
Account lockout interval	Period during which a locked user account cannot log in.

Migrate VMware Cloud Director Tenant Storage

Using the VMware Cloud Director Service Provider Admin Portal, you can migrate all vApps, independent disks, and catalog items of one or more organizations from one or more datastores to different datastores.

Before you decommission a datastore, you must migrate all the items stored on that datastore to a new datastore. You might also want to migrate an organization to a new datastore that has more storage capacity or uses a newer storage technology such as VMware vSAN.

Important Tenant storage migration is a resource-intensive operation that can run for a long time, especially when there are many assets to migrate. For more information about migrating tenant storage, see https://kb.vmware.com/kb/2151086.

The following table describes what happens if attached named disks or media are on the datastore that you want to migrate.

Table 7-1. Named Disk and Media Migration

Option	Description
Named disk attached to a VM	When a named disk is attached to a VM, it becomes part of the hard disk. VMware Cloud Director migrates the named disk as part of the VM migration. **Note** When you detach this disk, it remains on the migrated datastore.
Standalone named disk (not attached to a VM)	VMware Cloud Director migrates the standalone named disk to the target datastore.
Shared named disk attached to a VM	VMware Cloud Director does not support the migration of shared named disks when they are attached to one or more VMs. You must detach the shared named disk before the migration. If you try to migrate a shared named disk attached to a VM, the migration fails.

Table 7-1. Named Disk and Media Migration (continued)

Option	Description
Standalone shared named disk (not attached to a VM)	VMware Cloud Director migrates the standalone shared named disk to the target datastore.
Media inserted to one or more VMs	VMware Cloud Director does not support the migration of media inserted to VMs. You must eject the media before the migration. If you try to migrate media inserted to VMs, the migration fails.
Standalone media (not inserted to one or more VMs)	VMware Cloud Director migrates the standalone media to the target datastore.

Prerequisites

- Determine the storage policies used by the organization VDCs of the target organizations. See Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center.
- For each storage policy containing a source datastore that you want to migrate, verify that there is at least one destination datastore to which to migrate. You can create destination datastores or use existing ones. For further information about determining the datastores in the storage policies used by the target organizations, see the *vSphere Storage* documentation.

Procedure

1. Log in to the VMware Cloud Director Service Provider Admin Portal as a **system administrator** or with a role that has the **Organization: Migrate Tenant Storage** right.
2. Start the **Migrate Tenant Storage** wizard.
   - Under **Cloud Resources**, select **Organizations** and click **Migrate Tenant Storage**.
   - Under **vSphere Resources**, select **Datastores** and click **Migrate Tenant Storage**.
3. Select one or more organizations with storage items that you want to migrate, and click **Next**.
4. Select one or more source datastores to migrate.

   The wizard lists all datastores in the system.
5. (Optional) To migrate in their entirety all the VMs which have components on the selected datastores, turn on the **Migrate Entire Virtual Machine** toggle.

   By default, VMware Cloud Director migrates only the components from the selected datastore. If you turn on the toggle, when a VM has two disks and you select only one for migration, VMware Cloud Director migrates also the inventory from the other disk to the new datastore.
6. Click **Next**.
7. Select one or more destination datastores, and click **Next**.
8. Review the **Ready to Complete** page, and click **Finish** to begin the migration.

Manage Quotas on the Resource Consumption of an Organization in VMware Cloud Director

You can manage the overall resource consumption limit of an organization. You can add, edit, and remove the organization's quotas on VMs, Tanzu Kubernetes clusters, CPU, memory, or storage.

For information about limiting the resources available to users or groups, see Manage the Resource Quotas of a User or Manage the Resource Quotas of a Group .

Prerequisites

Create a VMware Cloud Director Organization.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 From the left panel, select **Organizations**.

3 Select the name of the organization for which you want to put on a quota.

4 Under the **Configure** section, select **Quotas** .

   Organizations do not have any quotas by default.

5 Click **Edit**.

6 Modify the quota for the selected organization.

   You can add, edit, or remove quotas on the number of Tanzu Kubernetes clusters, all or running VMs in the organization, consumed CPU, memory, and storage. Select **Unlimited** if you want the organization to have unlimited resources of the selected type.

7 Click **Save**.

Control Tenant Access to Resource Reservation Information in VMware Cloud Director

You can control user access to information about the resource consumption of VMware Cloud Director organizations in your environment.

Users with the **Organization vDC: View** right are not assigned the **Organization vDC: View Organization VDC Memory and CPU Reservation** right. As a **system administrator**, you can provide tenants with access to resource reservation information by adding this right to global tenant roles and to rights bundles in your environment.

Modify the Access of a Global Role to Resource Reservation Information in VMware Cloud Director

You can modify tenant access to resource reservation information by removing or adding a specific right to global tenant roles in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Global Roles**.

3 Click the name of the role that you want to modify.

4 Click **Edit**.

5 Depending on your VMware Cloud Director version, select one of the options.

Option	Description
For VMware Cloud Director 10.3.2	To provide access to resource reservation information, select the **Organization vDC: View Organization VDC Memory and CPU Reservation** right.
For VMware Cloud Director 10.3.1	To restrict the access to resource information, deselect the **Organization vDC: View Organization VDC Memory and CPU Reservation** right.

6 Click **Save**.

Modify the Access to Resource Reservation Information from a Rights Bundle in VMware Cloud Director

You can modify tenant access to resource reservation information by editing a tenant rights bundle in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Select the rights bundle that you want to modify.

4 Click **Edit**.

5 Depending on your VMware Cloud Director version, select one of the options.

Option	Description
For VMware Cloud Director 10.3.2	To provide access to resource reservation information, select the **Organization vDC: View Organization VDC Memory and CPU Reservation** right.
For VMware Cloud Director 10.3.1	To restrict the access to resource information, deselect the **Organization vDC: View Organization VDC Memory and CPU Reservation** right.

6 Click **Save**.

Manage the IP Spaces for a VMware Cloud Director Organization

You can manage the IP spaces that are available to a specific organization in your VMware Cloud Director environment.

If an IP space that is available to an organization is either shared or public, you can edit the floating IP addresses and prefixes that are available to the organization.

Prerequisites

- Verify that your role includes the **System IP Spaces:View** and **System IP Spaces:Manage** rights.
- Verify that the IP space that you want to edit is either shared or public.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 From the left panel, select **Organizations**.

3 Select the name of the organization for which you want to view the IP spaces.

4 Under IP Management, click **IP Spaces**.

A list of the IP spaces available to the organization appears.

5 Select the IP space that you want to edit and click **Manage Quota**.

6 (Optional) To edit the floating IPs quota, choose one of the following.

Option	Description
Activate Floating IPs	a Toggle on the **Floating IPs** option to activate it. b Enter a number of floating IPs to allocate to the IP space.
Deactivate Floating IPs	Toggle off the **Floating IPs** option to deactivate it, or select the **Unlimited** check box.

7 (Optional) To edit the IP prefixes available to the organization, choose one of the following.

Option	Description
Activate an IP prefix	a Toggle on an **IP prefix** option to activate it. b Enter a number of prefixes that you want to allocate, or select the **Unlimited** check box.
Deactivate an IP prefix	Toggle off the **Prefix** option to deactivate it.

8 Click **Save**.

Managing Organization Virtual Data Centers in VMware Cloud Director

8

To provide resources to a VMware Cloud Director organization, you create one or more organization virtual data centers (VDCs) for this organization. After you create an organization VDC, you can modify its properties, deactivate or delete it, and manage its allocation model, storage, and network settings.

Read the following topics next:

- Understanding Allocation Models in VMware Cloud Director
- Understanding VM Sizing, VM Placement, and vGPU Policies in VMware Cloud Director
- Using Kubernetes with Your VMware Cloud Director
- Understanding Trusted Platform Module Devices in VMware Cloud Director
- Create an Organization Virtual Data Center in VMware Cloud Director
- Activate or Deactivate an Organization Virtual Data Center in VMware Cloud Director
- Delete an Organization Virtual Data Center From VMware Cloud Director
- Modify the Name and the Description of an Organization Virtual Data Center in VMware Cloud Director
- Modify the Allocation Model Settings of an Organization Virtual Data Center in VMware Cloud Director
- Modifying the Storage Settings of an Organization Virtual Data Center in VMware Cloud Director
- Edit the Network Settings of a VMware Cloud Director Organization Virtual Data Center
- Set a Segment Profile Template for a VMware Cloud Director Organization VDC
- Assign an Edge Cluster to a VMware Cloud Director Organization Virtual Data Center
- Configuring Cross-Virtual Data Center Networking in VMware Cloud Director
- Modify the Metadata for a VMware Cloud Director Organization Virtual Data Center
- View the Resource Pools of a VMware Cloud Director Organization Virtual Data Center
- Managing the Distributed Firewall on a VMware Cloud Director Organization Virtual Data Center

Understanding Allocation Models in VMware Cloud Director

An allocation model determines how and when the allocated provider virtual data center (VDC) compute and memory resources are committed to the organization VDC in VMware Cloud Director.

The following table shows the vSphere resource distribution settings at the virtual machine (VM) or resource pool level based on the organization VDC allocation model.

	Flex Allocation Model	Elastic Allocation Pool Model	Non-Elastic Allocation Pool Model	Pay-As-You-Go Model	Reservation Pool Model
Elastic	Based on the organization VDC configuration.	Yes	No	Yes	No
vCPU Speed	If a VM CPU limit is not defined in a VM sizing policy, vCPU speed might impact the VM CPU limit within the VDC.	Impacts the number of running vCPUs in the Organization VDC.	Not Applicable	Impacts VM CPU Limit	Not Applicable
Resource Pool CPU Limit	Organization VDC CPU limit apportioned based on the number of VMs in the resource pool.	Organization VDC CPU allocation	Organization VDC CPU allocation	Unlimited	Organization VDC CPU allocation
Resource Pool CPU Reservation	Organization VDC CPU reservation is apportioned based on the number of vCPUs in the resource pool. Organization VDC CPU reservation equals the organization VDC CPU allocation times the CPU guarantee.	Sum of powered on VMs and equals the CPU guarantee times the vCPU speed, times the number of vCPUs.	Organization VDC CPU allocation times the CPU guarantee	None, expandable	Organization VDC CPU allocation
Resource Pool Memory Limit	Organization VDC memory limit is apportioned based on the number of VMs in the resource pool.	Unlimited	Organization VDC RAM allocation	Unlimited	Organization VDC RAM allocation
Resource Pool Memory Reservation	Organization VDC RAM reservation is apportioned based on the number of VMs in the resource pool. The organization VDC RAM reservation equals the organization VDC RAM allocation times the RAM guarantee.	Sum of RAM guarantee times vRAM of all powered-on VMs in the resource pool. The resource pool RAM reservation is expandable.	Organization VDC RAM allocation times the RAM guarantee	None, expandable	Organization VDC RAM allocation
VM CPU Limit	Based on the VM sizing policy of the VM.	Unlimited	Unlimited	vCPU speed times the number of vCPUs	Custom

	Flex Allocation Model	Elastic Allocation Pool Model	Non-Elastic Allocation Pool Model	Pay-As-You-Go Model	Reservation Pool Model
VM CPU Reservation	Based on the VM sizing policy of the VM.	0	0	Equals the CPU speed times the vCPU speed, times the number of vCPUs.	Custom
VM RAM Limit	Based on the VM sizing policy of the VM.	Unlimited	Unlimited	vRAM	Custom
VM RAM Reservation	Based on the VM sizing policy of the VM.	0	Equals vRAM times RAM guarantee plus RAM overhead.	Equals vRAM times RAM guarantee plus RAM overhead.	Custom

The non-flex VDC allocation models are legacy models. The legacy models are:

- Reservation Pool Model
- Allocation Pool Models
- Pay-As-You-Go Model

Converting a Legacy VDC Allocation Model to a Flex Allocation Model

The Flex Allocation Model provides full flexibility to control CPU and memory consumption at the VDC and individual VM levels, supports all allocation configurations, and can replace the legacy models. Unlike legacy models, the Flex Allocation Model is compatible with all values of a VDC compute policy.

You can add a VM placement and a VM sizing policy to a VDC with an elastic allocation pool model, non-elastic allocation pool model, pay-as-you-go model, or reservation pool model. Using the VMware Cloud Director GUI, if you add a VM placement or VM sizing policy to a VDC and the policy is not compatible with the existing VDC allocation model, a dialog box appears with a notification and the option to convert the VDC to a flex organization VDC. You can also use the VMware Cloud Director API by running a PUT request on the organization VDC and change the VDC `AllocationModel` to `Flex`.

VM Policy Compliance

Legacy VDC conversion does not cause VM non-compliance. If an administrator changes the VM compute values or VM group membership of a VM directly in the vCenter Server instance, a VM can become non-compliant with the assigned VM sizing or VM placement policy. A VM can also become non-compliant if a user with the necessary privileges changes the VM reservation and limit values by using the VMware Cloud Director API. If there is a non-compliant VM, VMware Cloud Director Tenant Portal UI displays a warning message. The tenant can see detailed information about the cause for the non-compliance and can make the VM compliant again, which reapplies the policies to the VM.

Suggested Use of the Allocation Models in VMware Cloud Director

Each allocation model can be used for different levels of performance control and management in VMware Cloud Director.

The following table contains information about the suggested use of each allocation model.

Allocation model	Suggested use
Flex allocation model	With the flex allocation model, you can achieve a fine-grained performance control at the workload level. By using the flex allocation model, VMware Cloud Director **system administrators** can manage the elasticity of individual organization VDCs. The flex allocation model uses policy-based management of workloads. With the flex allocation model, **cloud providers** can have a better control over memory overhead in an organization VDC and can enforce a strict burst capacity use for tenants.
Allocation pool allocation model	Use the allocation pool allocation model for long lived, stable workloads, where tenants subscribe to a fixed compute resource consumption and where **cloud providers** can predict and manage the compute resource capacity. The allocation pool allocation model is optimal for workloads with diverse performance requirements. With the allocation pool allocation model, all workloads share the allocated resources from the resource pools of vCenter Server. Regardless if you activate or deactivate elasticity, tenants receive a limited amount of compute resources. With the allocation pool allocation model, **cloud providers** activate or deactivate the elasticity at the system level and the setting applies to all allocation pool organization VDCs. If you use the non-elastic allocation pool allocation, the organization VDC pre-reserves the VDC resource pool and tenants can overcommit vCPUs but cannot overcommit any memory. If you use the elastic pool allocation, the organization VDC does not pre-reserve any compute resources and capacity can span through multiple clusters. Cloud providers manage the overcommitment of physical compute resources and tenants cannot overcommit vCPUs and memory.
Pay-as-you-go	Use the pay-as-you-go model when you do not have to allocate compute resources in vCenter Server upfront. Reservation, limit, and shares are applied on every workload that tenants deploy in the VDC. With the pay-as-you-go allocation model, every workload in the organization VDC receives the same percentage of the configured compute resources reserved. To VMware Cloud Director, the CPU speed of every vCPU for every workload is the same and you can only define the CPU speed at the organization VDC level. From a performance perspective, because you cannot change reservation settings of individual workloads, every workload receives the same preference. Pay-as-you-go allocation model is optimal for tenants that need workloads with different performance requirements to run within the same organization VDC. Because of the elasticity, the pay-as-you-go model is suitable for generic, short lived workloads that are part of autoscaling applications. With pay-as-you-go, tenants can match spikes in compute resources demand within an organization VDC.
Reservation pool	Use the reservation pool allocation model when you need a fine-grained control over the performance of workloads that are running in the organization VDC. From a **cloud provider** perspective, the reservation pool allocation model requires an upfront allocation of all compute resources in vCenter Server. The reservation pool allocation model is not elastic. The reservation pool allocation model is optimal for workloads that run on hardware that is dedicated to a specific tenant. In such cases, tenant users can manage use and overcommitment of compute resources.

Flex Allocation Model in VMware Cloud Director

VMware Cloud Director **system administrators** can create organization virtual data centers (VDC) by using the Flex allocation model. With the combination of Flex allocation and VM sizing policies, **system administrators** can control the CPU and RAM consumption at both the VDC and the individual virtual machine (VM) levels. The Flex allocation model supports all allocation configurations that are available in the existing allocation models.

You can convert all non-Flex organization VDCs into Flex VDCs by using the Service Provider Admin Portal, to publish an incompatible compute policy to the non-Flex organization VDC.

Note By using the VMware Cloud Director API, you can convert the allocation model of any organization VDC.

When creating a Flex organization VDC, **system administrators** control the following parameters of the organization VDC:

Parameter	Description
`Elasticity`	Activate or deactivate the elastic pool feature.
`Include VM Memory Overhead`	Include or exclude memory overhead in this VDC. When set to true, you might not be able to use the full capacity of the VDC because the memory overhead of every powered-on VM is also taken from the available capacity of the VDC. When set to false, the memory overhead is taken from the provider VDC and not from the allocated capacity of the VDC.
`CPU allocation`	The amount of CPU allocated to this VDC in MHz or GHz. The CPU allocation defines the CPU capacity of the VDC. The total CPU used by all VMs running in the VDC cannot exceed this value.
`CPU limit`	The CPU limit defines the CPU quota of a VDC. In most cases, the CPU limit is equal to the allocated CPU capacity of the VDC. Sometimes, you might be required not to allocate any CPU to the VDC, as in the pay-as-you-go model. In this case, you must set a quota on the overall CPU consumption by setting the CPU allocation to zero and the CPU limit to a non-zero value. You might also use this setting to allow an unlimited CPU quota. If set to unlimited, the backing resource pools of the VDC in vCenter Server get unlimited CPU.
`CPU resources guaranteed`	The percentage of CPU allocation that is physically reserved for the VDC.
`vCPU speed`	The default vCPU speed for VMs in the VDC.
`Memory allocation`	The amount of memory allocated to this VDC in MB or GB. This parameter defines the total memory capacity of the VDC. The total configured memory by all VMs running in the VDC cannot exceed this value.

Parameter	Description
`Memory limit`	The maximum amount of memory for this VDC in MB or GB. In most cases, the memory limit is the same as the memory allocation. In a non-elastic VDC, VMware Cloud Director uses this amount as a memory limit on the resource pool backing this VDC in vCenter Server. For elastic VDCs, VMware Cloud Director distributes this amount to all resource pools and applies it as a resource pool memory limit. The memory limit must be higher than the memory allocation when you create a VDC with 100 percent memory reservation and the `Include VM Memory Overhead` setting is false. In this case, if the memory limit is the same as the memory allocation, some VMs might not power on because vCenter Server does not allow the total memory requirement of the resource pool to expand beyond the value set in the memory limit.
`Memory resources guaranteed`	The percentage of memory allocation that is physically reserved for the VDC.
`Maximum number of VMs`	The maximum number of VMs in the VDC.

As a **VMware Cloud Director system administrator**, you can configure a Flex organization VDC to be elastic or non-elastic. When Flex organization VDCs have the elastic pool feature enabled, the organization VDC spans and uses all resource pools that are associated with its provider VDC. In VMware Cloud Director 9.7, if you convert a non-elastic organization VDC to an elastic organization VDC, you cannot convert the same organization VDC back to a non-elastic.

The Flex allocation model supports the capabilities of VM sizing policies without any constraints that other allocation models have. In the Flex allocation model, the VM compute resource allocation depends on the VM sizing policies. If you do not define a VM sizing policy for an organization VDC, the compute resource allocation depends on the organization VDC allocation model. Using the combination of the Flex allocation model and the organization VM sizing policies, a single organization VDC can accommodate VMs that use configuration that is common for all other allocation models. For more information, see Understanding VM Sizing, VM Placement, and vGPU Policies in VMware Cloud Director.

To create a Flex organization VDC, you can use the VMware Cloud Director Service Provider Admin Portal or the VMware Cloud Director API. For information about VMware Cloud Director API, see the *VMware Cloud Director API Programming Guide*.

Allocation Pool Allocation Model in VMware Cloud Director

In VMware Cloud Director, with the allocation pool allocation model, a percentage of the resources you allocate from the provider virtual data center (VDC) are committed to the organization VDC.

You can specify the percentage for both CPU and memory. This percentage is known as the percentage guarantee factor, and it allows you to overcommit resources.

As a system administrator, you can configure allocation-pool organization VDCs to be elastic or non-elastic. Elasticity is a global setting that affects all allocation-pool organization VDCs. See Modify VMware Cloud Director General System Settings.

By default, allocation-pool organization VDCs have an elastic allocation pool enabled. Systems upgraded from VMware Cloud Director 5.1 that have allocation-pool organization VDCs with virtual machines spanning multiple resource pools have elastic allocation pool enabled by default.

When allocation-pool VDCs have the elastic allocation pool feature enabled, the organization VDC spans and uses all resource pools associated with its provider VDC. As a result, vCPU frequency is now a mandatory parameter for an allocation pool.

Set the vCPU frequency and percentage guarantee factor in such a way that enough virtual machines can be deployed on the organization VDC without CPU being a bottleneck factor.

When a virtual machine is created, the placement engine places it on a provider VDC resource pool that best fits the requirements of the virtual machine. A subresource pool is created for this organization VDC under the provider VDC resource pool, and the virtual machine is placed under that subresource pool.

When the virtual machine powers on, the placement engine checks the provider VDC resource pool to ensure that it still can power on the virtual machine. If not, the placement engine moves the virtual machine to a provider VDC resource pool with sufficient resources to run the virtual machine. A subresource pool for the organization VDC is created if one does not exist.

The subresource pool is configured with sufficient resources to run the new virtual machine. The subresource pool's memory reservation is increased by the virtual machine's configured memory size times the percentage guarantee factor for the organization VDC. The subresource pool's CPU reservation is increased by the number of vCPU configured for the virtual machine times the vCPU specified at the organization VDC level times the percentage guarantee factor for CPU set at the organization VDC level. If the elastic allocation pool feature is enabled, the subresource pool's memory limit is increased by the virtual machine's configured memory size, and the subresource pool's CPU limit is increased by the number of vCPUs that the virtual machine is configured with times the vCPU frequency specified at the organization VDC level. The virtual machine is reconfigured to set its memory and CPU reservation to zero and the virtual machine placement engine places the virtual machine on a provider VDC resource pool.

With the elastic allocation pool allocation model, the limits are monitored and managed by VMware Cloud Director only. If the elastic feature is deactivated, the resource pool limit is set additionally.

The benefits of the allocation-pool model are that a virtual machine can take advantage of the resources of an idle virtual machine on the same subresource pool. This model can take advantage of new resources added to the provider VDC.

In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power-on because of a lack of resources on the original resource pool. This change might involve a minor cost to move the virtual machine disk files to a new resource pool.

When the elastic allocation pool feature is deactivated, the behavior of allocation-pool organization VDCs is similar to the allocation pool model in VMware Cloud Director 1.5. In this model, the vCPU frequency is not configurable. Overcommitment is controlled by setting the percentage of resources guaranteed.

By default, in an allocation pool VDC, virtual machines obtain their reservation, limit, and shares settings from the settings of the VDC. To create or reconfigure a virtual machine with custom resource allocation settings for both CPU and memory, you can use the vCloud API. See *VMware Cloud Director API Programming Guide*.

Pay-As-You-Go Allocation Model in VMware Cloud Director

With the VMware Cloud Director pay-as-you-go allocation model, resources are committed only when users create vApps in the organization VDC. You can specify a percentage of resources to guarantee, which allows you to overcommit resources. You can make a pay-as-you-go organization VDC elastic by adding multiple resource pools to its provider VDC.

Resources committed to the organization are applied at the virtual machine level.

When a virtual machine is powered on, if the original resource pool cannot accommodate the virtual machine, the placement engine checks the resource pool and assigns the virtual machine to another resource pool. If a subresource pool is not available for the resource pool, VMware Cloud Director creates one with an infinite limit and zero rate. The virtual machine's rate is set to its limit times its committed resources, and the virtual machine placement engine places the virtual machine on a provider VDC resource pool.

The benefit of the pay-as-you-go model is that it can take advantage of new resources added to the provider VDC.

In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power-on because of a lack of resources on the original resource pool. This change might involve a minor cost to move the virtual machine disk files to a new resource pool.

In the pay-as-you-go model, no resources are reserved ahead of time, so a virtual machine might fail to power on if there are not enough resources. Virtual machines operating under this model cannot take advantage of the resources of idle virtual machines on the same subresource pool, because resources are set at the virtual machine level.

By default, in a pay-as-you-go VDC, virtual machines obtain their reservation, limit, and shares settings from the settings of the VDC. To create or reconfigure a virtual machine with custom resource allocation settings for both CPU and memory, you can use the vCloud API. See *VMware Cloud Director API Programming Guide*.

Reservation Pool Allocation Model in VMware Cloud Director

With the reservation pool allocation model, all the resources you allocate are immediately committed to the VMware Cloud Director organization VDC. Users in the organization can control the overcommitment by specifying reservation, limit, and priority settings for individual virtual machines.

Because only one resource pool and one subresource pool are available in this model, the placement engine does not reassign a virtual machine's resource pool when it is powered on. The virtual machine's rate and limit are not modified.

With the reservation pool model, sources are always available when needed. This model also offers fine control over the virtual machine rate, limit, and shares, which can lead to optimal use of the reserved resources if you plan carefully.

In this model, reservation is always done at the primary cluster. If sufficient resources are not available to create an organization VDC on the primary cluster, the organization VDC creation fails.

Other limitations of this model are that it is not elastic and organization users might set non-optimal shares, rates, and limits on virtual machines, leading to underuse of resources.

Understanding VM Sizing, VM Placement, and vGPU Policies in VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, you can control the virtual machine (VM) resource allocation and placement on a specific cluster or host by using VM sizing policies, VM placement policies, and vGPU policies.

VMware Cloud Director **system administrators** create and manage VM sizing, VM placement, and vGPU policies at a global level and can publish individual policies to one or more organization virtual data centers (VDCs). Additionally, if a user saves a vApp as a vApp template to a catalog, the template also includes the vGPU, placement, and sizing policies of the original vApp as unmodifiable tagged policies.

When you publish a policy to an organization VDC, the policy becomes available to the users in the organization. When creating and managing VMs in the organization VDC, tenants can assign the available policies to the VMs. Tenants and users in the organization VDC cannot look into the specific configuration of a policy.

VM placement, VM sizing, and vGPU policies are a mechanism for cloud providers to define and offer differentiated levels of service, for example, a CPU intensive profile or a high memory usage profile. If you publish multiple VM placement, VM sizing, and vGPU policies to an organization VDC, tenant users can select between all custom policies and the default policy when creating and managing VMs in the organization VDC. The System Default policy is auto-generated for every VDC. You can delete the System Default policy in the VDC and mark another custom policy as the default. Every VDC must have a default compute policy. You can set as a default policy of a VDC any of the three compute policy types. The automatically generated System Default policy does not define any values and allows all virtual machine configurations.

VM placement policy

A VM placement policy defines the placement of a virtual machine on a host or group of hosts. It is a mechanism for **cloud provider administrators** to create a named group of hosts within a provider VDC. The named group of hosts is a subset of hosts within the provider VDC clusters that might be selected based on any criteria such as performance tiers or licensing. You can expand the scope of a VM placement policy to more than one provider VDC.

A VM placement policy defines VM-host affinity rules that directly impact the placement of tenant workloads. Administrators define or expose named host groups by using VM groups in vCenter Server. A VM group has a direct affinity to a host group and represents the host group to which it has the affinity.

You define the VM placement policy at the provider VDC level. A VM placement policy includes the following attributes:

- Name (must be unique in the provider VDC)
- Description
- A set of one or more VM groups selected from the underlying clusters in the provider VDC. You can select one VM group per cluster

A VM placement policy is optional during the creation of a virtual machine and a tenant can assign only one VM placement policy to a virtual machine.

When a tenant creates a virtual machine in the organization VDC and selects the VM placement policy, VMware Cloud Director adds the virtual machine to the VM group or VM groups that are referenced in the policy. As a result, VMware Cloud Director creates the virtual machine on the appropriate host.

A VM placement policy can have zero or one VM group from each cluster. For example, the VM placement policy *oracle_license* can comprise VM groups *oracle_license1* and *oracle_license2*, where VM group *oracle_license1* belongs to cluster *oracle_cluster1*, and VM group *oracle_license2* belongs to cluster *oracle_cluster2*.

When you assign a VM placement policy to a virtual machine, the placement engine adds this virtual machine to the corresponding VM group of the cluster on which it resides. For example, if you select to deploy a virtual machine on cluster *oracle_cluster1* and assign the VM placement policy *oracle_license* to this virtual machine, the placement engine adds the virtual machine to VM group *oracle_license1*.

VM sizing policy

A VM sizing policy defines the compute resource allocation for virtual machines within an organization VDC. The compute resource allocation includes CPU and memory allocation, reservations, limits, and shares.

With VM sizing policies, VMware Cloud Director **system administrators** can control the following aspects of compute resources consumption at the virtual machine level:

- Number of vCPUs and vCPU clock speed

- Amount of memory allocated to the virtual machine
- Memory and CPU reservation, limit, and shares
- Extra Configurations.

  The `extraConfigs` API parameter represents a mapping between a key and value pairs that are applied as extra configuration values on a virtual machine. You can create a policy with extra configurations only by using the vCloud API. Existing extra configurations appear in the Service Provider Admin Portal UI under **Extra Configurations** in the detailed VM sizing policy view.

You define the VM sizing policies at a global level. For more information about the VM sizing policy attributes, see Attributes of VM Sizing Policies in VMware Cloud Director.

VMware Cloud Director generates a default VM sizing policy for all VDCs. The default VM sizing policy contains only a name and description, and all remaining policy attributes are empty.

You can also define another VM sizing policy as the default policy for an organization VDC. The default VM sizing policy controls the resource allocation and consumption of the virtual machines that tenants create in the organization VDC, unless a tenant assigns another specific VM sizing policy to the virtual machine.

To limit the maximum compute resources that tenants can allocate to individual virtual machines within an organization VDC, cloud providers can define a maximum VM sizing policy. When assigned to an organization VDC, the maximum VM sizing policy acts as an upper bound for the compute resource configuration for all virtual machines within the organization VDC. The maximum VM sizing policy is not available to tenant users when creating a virtual machine. When you define a VM sizing policy as the maximum policy, VMware Cloud Director copies internally the content of the policy and uses the copied content as the maximum VM sizing policy. As a result, the organization VDC does not depend on the initially used VM sizing policy.

By using VM sizing policies, cloud providers can restrict the compute resources consumption for all virtual machines within an organization VDC to, for example, three predefined sizes, *Small Size*, *Medium Size*, and *Large Size*. The workflow is the following.

1. A **system administrator** creates three VM sizing policies with the following attributes.

Name	Attributes
Small Size	■ Description: Small-sized VM policy ■ Name: Small Size ■ Memory: 1024 ■ Number of vCPUs: 1
Medium Size	■ Description: Medium-sized VM policy ■ Name: Medium Size ■ Memory: 2048 ■ Number of vCPUs: 2
Large Size	■ Description: Large-sized VM policy ■ Name: Large Size ■ Memory: 4096 ■ Number of vCPUs: 4

2. Publish the new VM sizing policies to an organization VDC.
3. Optionally define one of the VM sizing policies as a default VM sizing policy for the organization VDC.

vGPU policy

Starting with VMware Cloud Director 10.3.2, you can create, manage, and publish vGPU policies. When creating a VM, tenant users can select between creating a VM for general purposes or a vGPU enabled VM that requires vGPU resources.

The vGPU policy defines the number of GPU PCI devices that a VM must have. A vGPU policy must have a vGPU profile and its count information. Optionally, you can add placement and sizing information to a vGPU policy.

A vGPU policy can define the placement of a VM on a host or group of hosts. It is a mechanism for **cloud provider administrators** to create a named group of hosts within a provider VDC. The named group of hosts is a subset of hosts within the provider VDC clusters that might be selected based on any criteria such as performance tiers or licensing. You can expand the scope of a vGPU policy to more than one provider VDC.

A vGPU policy defines VM-host affinity rules that directly impact the placement of tenant workloads. Administrators define or expose named host groups by using VM groups in vCenter Server. A VM group has a direct affinity to a host group and represents the host group to which it has the affinity.

You define the vGPU policy at the global or provider VDC level. A vGPU policy includes the following attributes:

- Name (unique globally)

  - Description
  - vGPU profile and its count

    VMware Cloud Director loads the available vGPU profiles from vCenter Server. When the PCI count is 1, a VM gets 1 vGPU PCI device, when the count is 2, a VM gets 2 vGPU PCI devices, and so on.
  - Provider VDC scope

    A vGPU policy can define its scope to all or a subset of provider VDCs in the system. For each provider VDC in the scope, the policy can further define the scope to one or more participating clusters of that provider VDC.
  - Host level placement

    A set of one or more VM groups selected from the underlying clusters in the provider VDC. You can select one VM group per cluster
  - Sizing information

    You can define the CPU and memory settings as part of a vGPU policy or during the creation of a VM, you can select a different available sizing policy.

  A vGPU policy is mandatory during the creation of a vGPU enabled VM, and a tenant can assign only one vGPU policy to a VM.

  When a tenant creates a VM in the organization VDC and selects the vGPU policy, VMware Cloud Director configures the VM to have vGPU PCI devices matching the vGPU profile and its count in the vGPU policy. VMware Cloud Director also adds the VM to the VM group or VM groups that are referenced in the policy. As a result, VMware Cloud Director creates the VM on the appropriate host.

  A vGPU policy can have zero or one VM group from each cluster. For example, the vGPU policy *oracle_license* can comprise VM groups *oracle_license1* and *oracle_license2*, where VM group *oracle_license1* belongs to cluster *oracle_cluster1*, and VM group *oracle_license2* belongs to cluster *oracle_cluster2*.

  When you assign a vGPU policy to a VM, the placement engine adds this VM to the corresponding VM group of the cluster on which it resides. For example, if you select to deploy a VM on cluster *oracle_cluster1* and assign the vGPU policy *oracle_license* to this VM, the placement engine adds the VM to VM group *oracle_license1*.

The available policy operations for cloud providers are the following:

- To define the placement of a VM on a host or group of hosts, create a placement policy. See Create a VM Placement Policy within a Provider VDC in VMware Cloud Director.
- To control the physical compute resource allocation for tenant workloads, create a sizing policy. See Create a VM Sizing Policy in VMware Cloud Director.
- To define the placement and compute resource allocation of a vGPU enabled VM, create a vGPU policy. See Create a vGPU Policy in VMware Cloud Director.

- Publish a policy to one or more organization VDCs. See Add a VM Placement Policy to an Organization VDC in VMware Cloud Director, Add a VM Sizing Policy to an Organization VDC in VMware Cloud Director, and Add a vGPU Policy to an Organization VDC in VMware Cloud Director.
- Set a VM placement policy, a VM sizing policy, or a vGPU policy as default.
- Edit a policy.
- Unpublish a policy from an organization VDC.
- Delete a policy. See Delete a VM Placement Policy From VMware Cloud Director, Delete a VM Sizing Policy From VMware Cloud Director, and Delete a vGPU Policy from VMware Cloud Director.

Users that have the **ORG_VDC_MANAGE_COMPUTE_POLICIES** right can create, update, and publish VM sizing, VM placement, and vGPU policies.

The following table lists the available VM sizing policy, VM placement, and vGPU policy operations for tenant users.

Table 8-1. VM Sizing Policy, VM Placement, vGPU Policy Operations for Tenant Users

Operation	Description
Assign a policy to a virtual machine during a virtual machine creation.	Tenant users that are authorized to create virtual machines in an organization VDC can optionally assign VM sizing, VM placement, and vGPU policies to VMs by using the VMware Cloud Director Tenant Portal. As a result, the parameters defined in a VM sizing policy control the CPU and memory consumption of the VM. The sizing parameters defined in a vGPU policy can also optionally control the CPU and memory consumption of the VM. Assigning a VM placement or sizing policy is not a requirement for tenants during a VM creation. If a tenant does not explicitly select a VM sizing policy to assign to a VM, the default VM sizing is applied to the virtual machine. If you do not create and publish any VM placement policies, the VM placement policy option is not visible to the tenants. If you do not create and publish any vGPU policies, the tenants can create only general purpose VMs. If a tenant selects a VM placement or vGPU policy that has sizing information, the VM sizing policy option becomes hidden to the tenant. You can create a VM placement policy with sizing information only by using the vCloud API. If there is only one VM sizing policy, the VM sizing policy option is not visible to the tenants. When the **system administrator** sets the **vCPU Count**, **Cores Per Socket**, and **Memory** attributes in a VM sizing or vGPU policy, if a tenant selects the policy, these values are shown, but not editable.
Assign a policy to an existing virtual machine.	Tenant users that are authorized to manage VMs in an organization VDC can assign or change the VM sizing, VM placement, and vGPU policies of an existing VM using the VMware Cloud Director Tenant Portal. When a tenant changes the VM placement or vGPU policy, the VM moves to a new host as per the VM-host affinity rule defined in the new policy. When a tenant changes a VM sizing policy or vGPU policy with defined sizing information, the system reconfigures the VM to consume compute resources as specified in the new policy.

The workflow for working with VM placement and VM sizing policies is the following.

1 You creates one or more VM placement policies. See Create a VM Placement Policy within a Provider VDC in VMware Cloud Director.

   When you create a VM placement policy to be scoped for a single provider VDC, the name of the VM placement policy must be unique within the provider VDC scope of the policy. If you create a VM placement policy scoping more than one provider VDC, the VM placement policy name becomes unique globally within the VMware Cloud Director site.

2 You create one or more VM sizing policies. See Create a VM Sizing Policy in VMware Cloud Director.

   The names of VM sizing policies are unique in a single VMware Cloud Director site.

3 You create one or more vGPU policies. See Create a vGPU Policy in VMware Cloud Director.

   The names of vGPU policies are unique in a single VMware Cloud Director site.

4 You publish the VM placement, VM sizing, and vGPU policies to one or more organization VDCs. See Add a VM Placement Policy to an Organization VDC in VMware Cloud Director, Add a VM Sizing Policy to an Organization VDC in VMware Cloud Director, and Add a vGPU Policy to an Organization VDC in VMware Cloud Director.

   Publishing a policy makes it available for tenant users in the organization VDCs during virtual machine creation and virtual machine editing.

5 When creating or updating a VM, tenants can use the VMware Cloud Director API or the VMware Cloud Director Tenant Portal to assign a VM sizing, VM placement, and vGPU policy to a VM.

Attributes of VM Sizing Policies in VMware Cloud Director

When you create a virtual machine (VM) sizing policy, by using VMware Cloud Director Service Provider Admin Portal, you can specify a subset of all available attributes. The only mandatory attribute is the VM sizing policy name.

There are two types of parameters in a VM sizing policy.

- Individual VM sizing configuration - You preconfigure the specified RAM, vCPU count, and cores per socket for the VMs under the current policy.
- Constraints on the maximum resources - You preconfigure a limitation for consumption of memory and CPU by a single VM under the current policy.

The following table lists all attributes that you can define within a VM sizing policy.

Table 8-2. VDC Compute Policy Attributes

VDC Compute Policy Attribute	API Parameter	Description
`Name`	`name`	Mandatory parameter that is used as an identifier for the VM sizing policy.
`Description`	`description`	Represents a short description of the VM sizing policy.

Table 8-2. VDC Compute Policy Attributes (continued)

VDC Compute Policy Attribute	API Parameter	Description
vCPU Speed	cpuSpeed	Defines the vCPU speed of a core in MHz or GHz.
vCPU Count	cpuCount	Defines the number of vCPUs configured for a VM. This is a VM hardware configuration. When a tenant assigns the VM sizing policy to a VM, this count becomes the configured number of vCPUs for the VM.
Cores Per Socket	coresPerSocket	The number of cores per socket for a VM. This is a VM hardware configuration. The number of vCPUs that is defined in the VM sizing policy must be divisible by the number of cores per socket. If the number of vCPUs is not divisible by the number of cores per socket, the number of cores per socket becomes invalid.
CPU Reservation Guarantee	cpuReservationGuarantee	Defines how much of the CPU resources of a VM are reserved. The allocated CPU for a VM equals the number of vCPUs times the vCPU speed in MHz. The value of the attribute ranges between 0 and one. Value of 0 CPU reservation guarantee defines no CPU reservation. Value of 1 defines 100% of CPU reserved.
CPU Limit	cpuLimit	Defines the CPU limit in MHz or GHz for a VM. If not defined in the VDC compute policy, CPU limit is equal to the vCPU speed multiplied by the number of vCPUs.
CPU Shares	cpuShares	Defines the number of CPU shares for a VM. Shares specify the relative importance of a VM within a virtual data center. If a VM has twice as many shares of CPU as another VM, it is entitled to consume twice as much CPU when these two virtual machines are competing for resources. If not defined in the VDC compute policy, normal shares are applied to the VM.
Memory	memory	Defines the memory configured for a VM in MB or GB. This is a VM hardware configuration. When a tenant assigns the VM sizing policy to a VM, the VM receives the amount of memory defined by this attribute.
Memory Reservation Guarantee	memoryReservationGuarantee	Defines the reserved amount of memory that is configured for a VM. The value of the attribute ranges between 0 and 100%.
Memory Limit	memoryLimit	Defines the memory limit in MB or GB for a VM. If not defined in the VM sizing policy, memory limit is equal to the allocated memory for the VM.

Table 8-2. VDC Compute Policy Attributes (continued)

VDC Compute Policy Attribute	API Parameter	Description
`Memory Shares`	`memoryShares`	Defines the number of memory shares for a VM. Shares specify the relative importance of a VM within a virtual data center. If a VM has twice as many shares of memory as another VM, it is entitled to consume twice as much memory when these two virtual machines are competing for resources. If not defined in the VDC compute policy, normal shares are applied to the VM.
`Extra Configurations`	`extraConfigs`	Represents a mapping between a key and value pairs that are applied as extra configuration values on a VM. You can create a policy with extra configurations only through the vCloud API. Existing extra configurations appear in the Service Provider Admin Portal UI under **Extra Configurations** in the detailed VM sizing policy view.

Creating and Managing vGPU Policies in VMware Cloud Director

Starting with VMware Cloud Director 10.3.2, you can create, manage, and publish vGPU policies to organization VDCs that use flex allocation model.

NVIDIA GRID vGPU is a graphics acceleration technology from NVIDIA that you can use to share a single graphics processing unit (GPU) among multiple virtual desktops. When you use NVIDIA GRID cards, installed on an x86 host, in a desktop and application virtualization solution running on vSphere 6.x and later, you can render application graphics with superior performance compared to non-hardware-accelerated environments. This capability is useful for graphics-intensive use cases such as designers in a manufacturing setting, architects, engineering labs, higher education, oil and gas exploration, clinicians in a healthcare setting, and for power users and knowledge workers who need access to rich 2D and 3D graphical interfaces.

Under **Infrastructure Resources**, you can view the **vGPU Profiles** that VMware Cloud Director loads from the vCenter Server clusters with virtual graphics processing unit (vGPU) capabilities. Each profile represents a type of vGPU. You can use a vGPU profile to create a vGPU policy that tenants can use for their virtual machines. NVIDIA vGPU profiles determine how many fixed share resources can be allocated to each VM from the total available memory.

You create and manage vGPU policies at the global or at the provider level. You can publish individual policies to one or more organization VDCs that use flex allocation model.

View and Manage vGPU Profile Information in VMware Cloud Director

When the hosts in a cluster backing the provider VDC resource pool have vGPU capabilities, VMware Cloud Director loads the vGPU profile information from vCenter Server. You can view, edit, and delete the vGPU profile information.

You select a vGPU profile during the creation of a vGPU policy. When you publish a vGPU policy, the vGPU profile names and instructions of the profiles you added to the policy become visible to the tenants.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vGPU Profiles**.
3. Click the radio button next to a vGPU profile name, and click **Edit**.
4. (Optional) Edit the tenant-facing name.
5. (Optional) Edit the tenant-facing instructions.

   You can provide additional instructions to your tenants, for example, you can provide a link to the NVIDIA GRID vGPU release notes document.
6. Click **Save**.
7. To delete a vGPU profile, click the radio button next to a vGPU profile name, and click **Delete**.

   The option to delete a vGPU profile appears for the vGPU profiles which the system detects as no longer valid in the underlying infrastructure and which are not used by any vGPU policies.
8. To view vGPU profile metrics for their use, click the name of the profile and under **Usage metrics** you can view details about where this profile is used.

   You can view the names of the VMs and vApps that use the vGPU profile, usage count, policy name, organization, and organization VDC information.

Create a vGPU Policy in VMware Cloud Director

Starting with VMware Cloud Director 10.3.2, to define the placement and sizing settings of VMs that require vGPU resources, you can create vGPU policies.

Prerequisites

Verify that at least one vCenter Server host has an NVIDIA graphics device attached and all required vSphere Installation Bundles (VIBs) are installed on the host.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. Navigate to the **Create a vGPU Policy** wizard.
   - In the left panel, select **vGPU Policies**, and click **New**.
   - a. In the left panel, select **Provider VDCs**.

     b. Click the name of a provider VDC with the NVIDIA icon indicating vGPU capabilities.

     c. Under **Policies**, select **vGPU**, and click **New**.
3. On the **General** page of the **Create vGPU Policy** wizard, enter a vGPU policy name, and optionally, a description.
4. Click **Next**.

5 Select a vGPU profile and PCI device count associated with this policy, and click **Next**.

   By selecting a count, you select the number of PCI devices that you can attach to a VM that you create by using this policy.

6 Select which provider VDC clusters can have access to the policy, and click **Next**.

   If you navigated to the wizard through the **Provider VDC** tab, only the selected provider VDC is visible. Selecting **No** creates a global vGPU policy that all provider VDC clusters can access.

7 If you want to define the placement of a VM on a host or group of hosts, select **Yes** and select one or more VM groups.

   A VM group has a direct affinity to a host group and represents the host group to which it has the affinity.

   You can select one VM group per cluster.

8 Click **Next**.

9 If you want to define the compute resource allocation for VMs, select **Yes**, and click **Next**.

   a Select the CPU allocation settings that you want to apply to the policy, and click **Next**.

   b Select the memory allocation settings that you want to apply to the policy, and click **Next**.

   Note The memory reservation guarantee must always be 100%.

   c Configure additional VM settings as `extraConfig` parameters, and click **Next**.

   The `Extra Configurations` VDC compute policy attribute is a mapping between key and value pairs applied as extra configuration values on a VM.

10 Review the vGPU policy settings, and click **Finish**.

Add a vGPU Policy to an Organization VDC in VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, when you create a vGPU policy, it is not visible to tenants. You can publish a vGPU policy to an organization VDC to make it available to tenants.

Publishing a vGPU policy to an organization VDC makes the policy visible to tenants. The tenant can select the policy when they create a new standalone VM or a VM from a template, edit a VM, add a VM to a vApp, and create a vApp from a vApp template. You cannot delete a vGPU policy that is available to tenants.

Prerequisites

- Verify that you have at least one organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.
- Verify that you have at least one vGPU policy. See Create a vGPU Policy in VMware Cloud Director.

- Verify that the organization VDC to which you want to publish a vGPU policy is using flex allocation model.
- Verify that the organization VDC to which you want to publish a vGPU policy belongs to a provider VDC scoped in the vGPU policy. Alternatively, verify that the vGPU policy you want to publish is global and does not have a provider VDC scope.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Select an organization VDC and under **Policies**, select the **vGPU** tab.
4. Click **Add**.
5. Select the vGPU policies that you want to add to the organization VDC, and click **OK**.

What to do next

- Select a policy and click **Remove** to unpublish the policy.
- Select a vGPU policy and click **Set as default** to make that policy appear as the default choice for the tenants during a VM and vApp creation and VM edit. If there is more than one vGPU policy published for an organization VDC, the tenant can select a different policy from the default one.

Delete a vGPU Policy from VMware Cloud Director

If a vGPU policy is not published to tenants, you can delete it from the provider VDC in VMware Cloud Director.

Prerequisites

- Verify that the vGPU policy is not added to an organization VDC. You cannot delete vGPU policies that are available to tenants.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click a provider VDC from the list.
4. Under **Policies**, select the **vGPU** tab, and select the radio button next to a vGPU policy.
5. Click **Delete**.

Create a VM Placement Policy within a Provider VDC in VMware Cloud Director

A VM placement policy is a VDC compute policy that contains a reference to a provider VDC policy in VMware Cloud Director. You can add multiple provider VDCs to the scope of a VM placement policy. You can use a VM placement policy to define the placement of a VM on a specific host, group of hosts, or a cluster.

A VM placement policy can contain a reference to one or more provider VDC policies. When you create a placement policy from within a provider VDC, the policy references only the selected provider VDC. You can include more provider VDCs in the scope of a VM placement policy by editing it or you can create a placement policy from the **VM Placement Policies** tab to include more than one provider VDC in its scope. See Edit a VM Placement Policy in VMware Cloud Director and Create a Global VM Placement Policy in VMware Cloud Director.

Prerequisites

- Verify that you have at least one provider VDC in your environment.
- Verify that you have at least one VM group in your environment.

  A VM group is a collection of VMs that you can link to a host group with positive affinities. Through a positive affinity rule, you cause the placement of a group of VMs on a specific host. You can create a VM group through the vCenter Server UI or the VMware Cloud Director API.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click a provider VDC from the list.
4. Click the **VM Placement Policies** tab and click **New**.
5. (Optional) On the **What is VM Placement policy** page of the wizard, select the check box to stop showing the VM placement policy information.
6. Click **Next**.
7. Enter a name for the VM placement policy and, optionally, a description.
8. Select the VM groups or logical VM groups to which you want the VM to be linked and click **Next**.

   When you select more than one logical group, if a tenant applies this policy to a VM, the VM becomes a member of all the VM groups included in the selected logical VM groups. The VM is conditioned to a combination of all the affinities that apply to the VMs in these groups. You can select simultaneously VM groups and logical groups.

   You can create an inline logical VM group by selecting one VM group per cluster. This logical VM group does not have a name and can be used only for the selected VM Placement policy.

9 For VMware Cloud Director 10.4.2 and later, if you want to define a sizing policy together with the placement policy and you are not reusing an existing policy, set predefined CPU and memory consumption constraints that apply to VMs with this policy.

   To learn more about the CPU and memory attributes, see Attributes of VM Sizing Policies in VMware Cloud Director.

   a Select **Yes**, and click **Next**.

   b On the **CPU** page, select the CPU allocation settings that you want to apply to the policy, and click **Next**.

   c Select the memory allocation settings that you want to apply to the policy, and click **Next**.

   d Configure additional VM settings as `extraConfig` parameters.

      The `Extra Configurations` VDC compute policy attribute is a mapping between key and value pairs applied as extra configuration values on a VM.

10 For VMware Cloud Director 10.4.2 and later, click **Next**.

11 Review the VM placement policy settings and click **Finish**.

What to do next

- Create a VM Sizing Policy in VMware Cloud Director.
- Add a VM Placement Policy to an Organization VDC in VMware Cloud Director.
- Starting with VMware Cloud Director 10.2.2, you can Edit a VM Placement Policy in VMware Cloud Director.
- Delete a VM Placement Policy From VMware Cloud Director.

Edit a VM Placement Policy in VMware Cloud Director

Starting with VMware Cloud Director 10.2.2, you can edit and change the scope of a VM placement policy.

Prerequisites

Create a Global VM Placement Policy in VMware Cloud Director

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 From the left panel, select **VM Placement Policies**.

3 Select a VM placement policy, and click **Edit**.

4 (Optional) On the **What is VM Placement policy** page of the wizard, select the check box to stop showing the VM placement policy information.

5 Click **Next**.

6 Edit the name for the VM placement policy and, optionally, the description.

7 Edit the VM groups and logical VM groups to which you want the VM to be linked and click **Next**.

   You can select one VM group per cluster. You cannot deselect clusters that are currently in use, for example, when you publish the placement policy to an organization VDC.

8 Review the VM placement policy settings and click **Finish**.

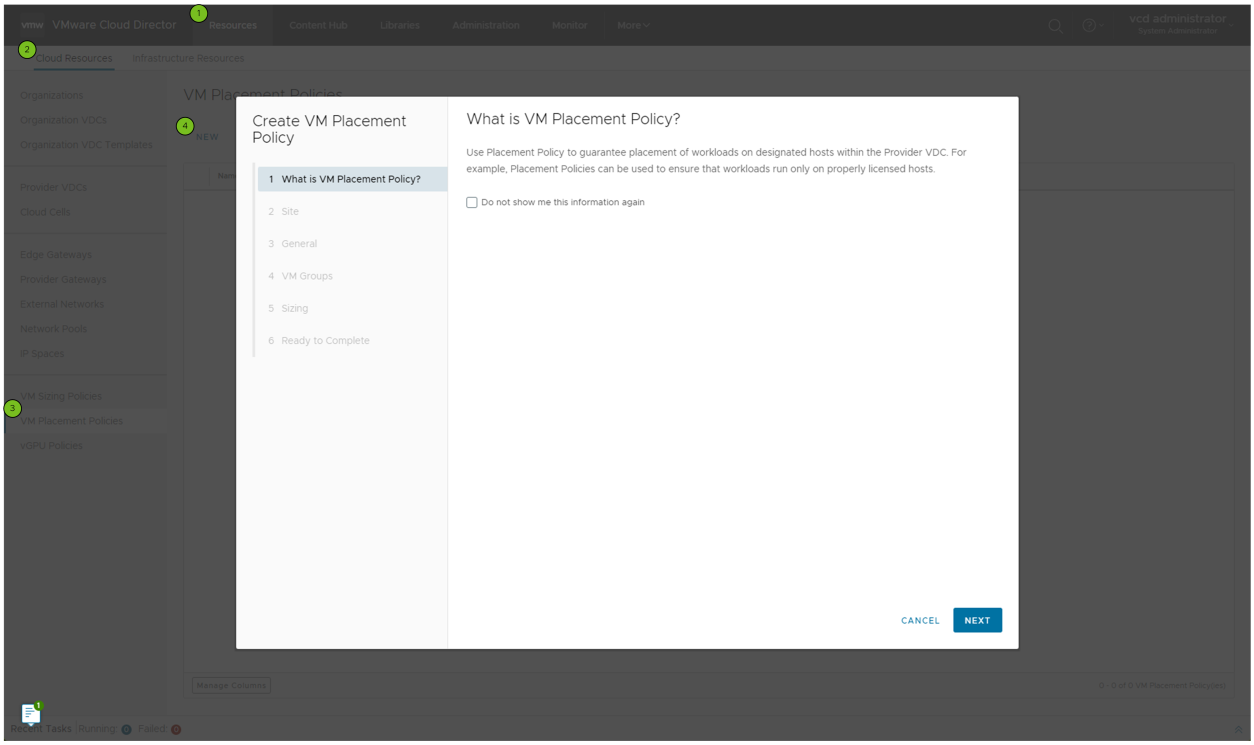
What to do next

- Create a VM Sizing Policy in VMware Cloud Director.
- Add a VM Placement Policy to an Organization VDC in VMware Cloud Director.
- Delete a VM Placement Policy From VMware Cloud Director.

Create a Global VM Placement Policy in VMware Cloud Director

A VM placement policy can contain a reference to one or more provider VDC policies in VMware Cloud Director. You can use a VM placement policy to define the placement of a VM on a specific host, group of hosts, or one or more clusters.

When you create a placement policy from within a provider VDC, the policy references only the selected provider VDC. See Create a VM Placement Policy within a Provider VDC in VMware Cloud Director. You can include more provider VDCs in the scope of a VM placement policy by editing it, or you can create a global placement policy.



Create VM Placement Policy

1 What is VM Placement Policy?

2 Site

3 General

4 VM Groups

5 Sizing

6 Ready to Complete

What is VM Placement Policy?

Use Placement Policy to guarantee placement of workloads on designated hosts within the Provider VDC. For example, Placement Policies can be used to ensure that workloads run only on properly licensed hosts.

☐ Do not show me this information again

Prerequisites

- Verify that you have at least one provider VDC in your environment.

- Verify that you have at least one VM group in your environment.

  A VM group is a collection of VMs that you can link to a host group with positive affinities. Through a positive affinity rule, you cause the placement of a group of VMs on a specific host. You can create a VM group through the vCenter Server UI or the VMware Cloud Director API.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. From the left panel, select **VM Placement Policies**, and click **New**.
3. (Optional) On the **What is VM Placement policy** page of the wizard, select the check box to stop showing the VM placement policy information.
4. Click **Next**.
5. Enter a name for the VM placement policy and, optionally, a description.
6. Select the VM groups and logical VM groups to which you want the VM to be linked and click **Next**.

   You can select one VM group per cluster.

   When you select more than one logical group, if a tenant applies this policy to a VM, the VM becomes a member of all the VM groups included in the selected logical VM groups. The VM is conditioned to a combination of all the affinities that apply to the VMs in these groups. You can select simultaneously VM groups and logical groups.

   You can create an inline logical VM group by selecting one VM group per cluster. This logical VM group does not have a name and can be used only for the selected VM Placement policy.
7. If you want to define a sizing policy together with the placement policy and you are not reusing an existing policy, set predefined CPU and memory consumption constraints that apply to VMs with this policy.

   To learn more about the CPU and memory attributes, see Attributes of VM Sizing Policies in VMware Cloud Director.

   a. Select **Yes**, and click **Next**.
   b. On the **CPU** page, select the CPU allocation settings that you want to apply to the policy, and click **Next**.
   c. Select the memory allocation settings that you want to apply to the policy, and click **Next**.
   d. Configure additional VM settings as `extraConfig` parameters.

      The `Extra Configurations` VDC compute policy attribute is a mapping between key and value pairs applied as extra configuration values on a VM.
8. Click **Next**.
9. Review the VM placement policy settings and click **Finish**.

What to do next

- Create a VM Sizing Policy in VMware Cloud Director.
- Add a VM Placement Policy to an Organization VDC in VMware Cloud Director.
- Edit a VM Placement Policy in VMware Cloud Director.
- Delete a VM Placement Policy From VMware Cloud Director.

Add a VM Placement Policy to an Organization VDC in VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, when you create a VM placement policy, it is not visible to tenants. You can publish a VM placement policy to an organization VDC to make it available to tenants.

Publishing a VM placement policy to an organization VDC makes the policy visible to tenants. To publish a placement policy to an organization VDC, you must first include its backing provider VDC in the scope of the VM placement policy by Create a Global VM Placement Policy in VMware Cloud Director or Edit a VM Placement Policy in VMware Cloud Director. The tenant can select the policy when they create a new standalone VM or a VM from a template, edit a VM, add a VM to a vApp, and create a vApp from a vApp template. You cannot delete a VM placement policy that is available to tenants.

Prerequisites

- Verify that you have at least one organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.
- Verify that you have at least one VM placement policy. See Create a VM Placement Policy within a Provider VDC in VMware Cloud Director. You can create a global placement policy that contains a reference to one or more provider VDC policies. See Create a Global VM Placement Policy in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Select an organization VDC and click the **VM Placement Policies** tab.

4 Click **Add**.

5 Select the VM placement policies that you want to add to the organization VDC and click **OK**.

What to do next

- Select a policy and click **Remove** to unpublish the policy.

- Select a VM placement policy and click **Set as default** to make that policy appear as the default choice for the tenants during a VM and vApp creation and VM edit. If there is more than one VM placement policy published for an organization VDC, the tenant can select a different policy from the default one.

Delete a VM Placement Policy From VMware Cloud Director

If a VM placement policy is not published to tenants, you can delete it from the provider VDC in VMware Cloud Director.

Prerequisites

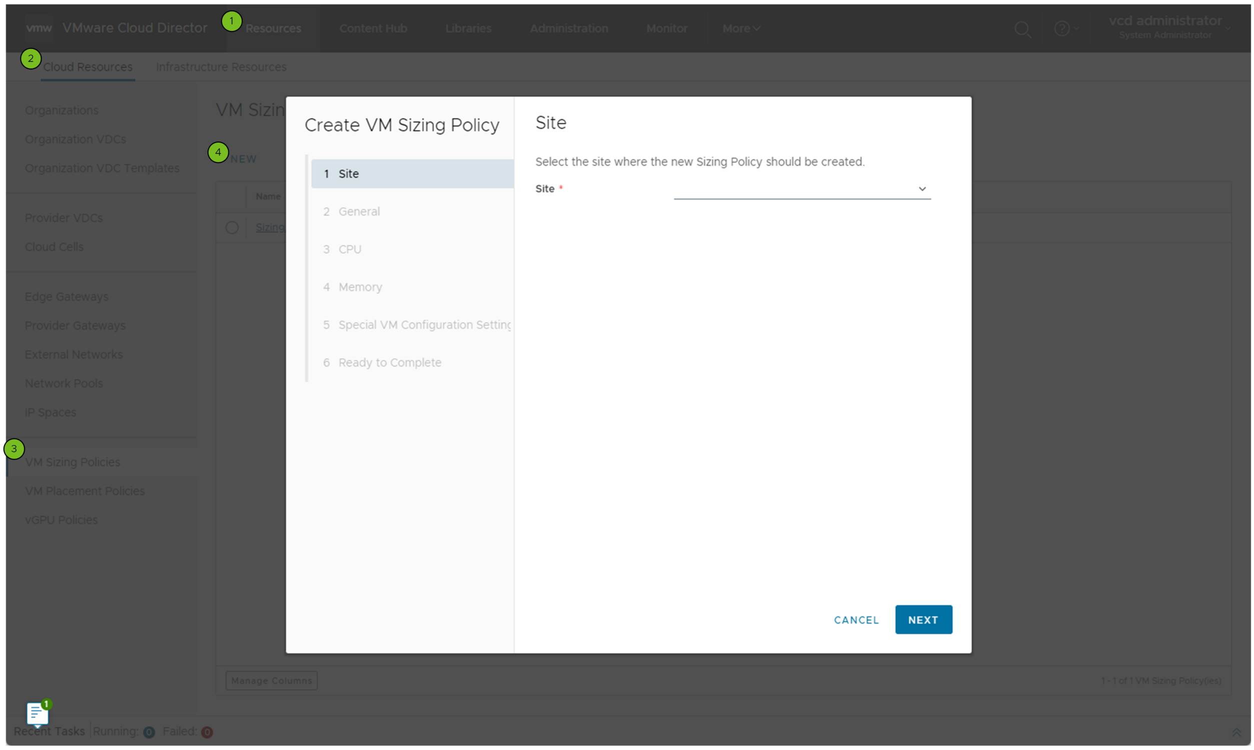
- Verify that you have at least one VM placement policy in your environment.
- Verify that the VM placement policy is not added to an organization VDC. You cannot delete VM placement policies that are available to tenants.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**.
3. Click a provider VDC from the list.
4. Click the **VM Placement Policies** tab and select a VM placement policy.
5. Click **Delete**.

Create a VM Sizing Policy in VMware Cloud Director

By using VMware Cloud Director Service Provider Admin Portal, you can create a VM sizing policy to make available to tenants predefined CPU and memory consumption constraints that they can apply to individual VMs in an organization VDC.



Site

Select the site where the new Sizing Policy should be created.

Site *

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **VM Sizing Policies**.

3 Click **New**.

4 Enter a name for the VM sizing policy, and optionally a description.

5 Click **Next**.

6 On the **CPU** page, select the CPU allocation settings that you want to apply to the policy and click **Next**.

7 Select the memory allocation settings that you want to apply to the policy and click **Next**.

8 (Optional) Configure additional VM settings as `extraConfig` parameters, and click **Next**.

The `Extra Configurations` VDC compute policy attribute is a mapping between key and value pairs applied as extra configuration values on a VM.

9 Review the VM sizing policy settings and click **Finish**.

What to do next

- After you create a VM sizing policy, you can edit only the VM sizing policy name and description. See Edit a VM Sizing Policy in VMware Cloud Director.
- Add a VM Sizing Policy to an Organization VDC in VMware Cloud Director.
- Create a VM Placement Policy within a Provider VDC in VMware Cloud Director.

Add a VM Sizing Policy to an Organization VDC in VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, when you create a VM sizing policy, it is not visible to tenants. You can publish VM sizing policy to an organization VDC to make it available to tenants.

Publishing a VM sizing policy to an organization VDC makes the policy visible to tenants. The tenant can select the policy when they create a new standalone VM or a VM from a template, edit a VM, add a VM to a vApp, and create a vApp from a vApp template. You cannot delete a VM sizing policy that is available to tenants.

Prerequisites

- Verify that you have at least one organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.
- Verify that you have at least one VM sizing policy. See Create a VM Sizing Policy in VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Select an organization VDC and click the **VM Sizing Policies** tab.
4. Click **Add**.
5. Select the VM sizing policies that you want to add to the organization VDC and click **OK**.

What to do next

- Select a policy and click **Remove** to unpublish the policy.
- Select a VM sizing policy and click **Set as default** to make that policy appear as the default choice for the tenants during a VM and vApp creation and VM edit. If there is more than one VM sizing policy published for an organization VDC, the tenant can select a different policy from the default one.

Edit a VM Sizing Policy in VMware Cloud Director

After you create a VM sizing policy, in VMware Cloud Director Service Provider Admin Portal, you can edit only its name and description. Editing the CPU and memory parameters is not supported.

Prerequisites

- Verify that you have at least one organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.

- Verify that you have at least one VM sizing policy. See Create a VM Sizing Policy in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **VM Sizing Policies**.

3 Click the name of the VM sizing policy you want to edit.

4 To edit the name and description of the policy, click **Edit**.

5 Click **Save**.

What to do next

Add a VM Sizing Policy to an Organization VDC in VMware Cloud Director

Delete a VM Sizing Policy From VMware Cloud Director

By using VMware Cloud Director Service Provider Admin Portal, you can delete VM sizing policies that are not published to tenants.

Prerequisites

- Verify that you have at least one VM sizing policy in your environment.
- Verify that the VM sizing policy is not added to an organization VDC. You cannot delete VM sizing policies that are available to tenants.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **VM Sizing Policies**.

3 Select a VM sizing policy and click **Delete**.

Using Kubernetes with Your VMware Cloud Director

By using Kubernetes with VMware Cloud Director, you can provide a multi-tenant Kubernetes service to your tenants.

For tenant information on working with Kubernetes clusters, see Working with Kubernetes Clusters in the VMware Cloud Director Tenant Portal.

VMware Cloud Director Container Service Extension

Kubernetes Container Clusters is the VMware Cloud Director Container Service Extension plug-in for VMware Cloud Director. To create Kubernetes clusters, service providers and tenants must use the Kubernetes Container Clusters plug-in. You can download the latest compatible Kubernetes Container Clusters plug-in from the VMware Cloud Director download page for the relevant VMware Cloud Director version, and upload the plug-in to the VMware Cloud Director Service Provider Admin Portal. To enable tenants to create Kubernetes clusters, you must publish the plug-in to the tenant organizations. For more information, see VMware Cloud Director Container Service Extension Documentation.

vSphere with Tanzu in VMware Cloud Director

You can use vSphere with Tanzu in VMware Cloud Director to create provider virtual data centers (VDCs) backed by Supervisor Clusters. A host cluster with enabled vSphere with Tanzu is called a Supervisor Cluster. You can set restrictions on the uses of the resources and limit the available resources, including number of Kubernetes clusters per organization, user, or group. For more information, see Manage Quotas on the Resource Consumption of an Organization in VMware Cloud Director.

To use vSphere with Tanzu in VMware Cloud Director, first, you must enable the vSphere with Tanzu functionality on a vSphere 7.0 or later cluster, and configure that cluster as a Supervisor Cluster. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation. The vCenter Server instance that you want to use can have both host clusters and Supervisor Clusters.

To create clusters, you must publish a provider VDC Kubernetes policy to an organization and apply the organization VDC Kubernetes policy during the creation.

VMware Tanzu® Kubernetes Grid™ Service Clusters

VMware Tanzu® Kubernetes Grid™ Service clusters, informally known as TKGS - You can use the vSphere with Tanzu runtime option to create vSphere with Tanzu managed Tanzu Kubernetes Grid Service clusters. Tanzu Kubernetes Grid Service supports VMware hardened and signed upstream compatible Kubernetes, multiple control plane nodes, First Class Disk-based dynamic and static provisioning of Persistent Volumes, and L4 load balancer automation. This option offers more features, however, it might be more expensive. For more information, see the *vSphere with Tanzu Configuration and Management* guide in the vSphere documentation.

Important To integrate Tanzu Kubernetes Grid Service with VMware Cloud Director, when configuring the supervisor cluster in vSphere, you must configure the NSX option.

Workflow for Tanzu Kubernetes Cluster Creation

1 Add a vCenter Server 7.0 or later instance with an enabled vSphere with Tanzu functionality to VMware Cloud Director. See Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director.

2 Verify the network settings on each Supervisor Cluster to enable them to run Kubernetes workloads.

Important The IP address ranges for the `Ingress CIDRs` and `Services CIDR` parameters must not overlap with IP addresses 10.96.0.0/12 and 192.168.0.0/16 which are the default vSphere values for the `services` and `pods` parameters. See the configuration parameters for Tanzu Kubernetes clusters information in the *vSphere with Kubernetes Configuration and Management* guide.

Note If you modify the network settings of the Supervisor Cluster after the initial setup, you must refresh the vCenter Server instance to adjust the automatic firewall policies and NAT rules that block the access to the Tanzu Kubernetes cluster from outside the organization virtual data center in which the cluster is created.

3 Create a provider VDC backed by a Supervisor Cluster. See Create a Provider Virtual Data Center in Your VMware Cloud Director.

Alternatively, you can add a Supervisor Cluster to an existing provider VDC. If you have a vSphere 6.7 or earlier environment, you can also upgrade the environment to version 7.0 and enable vSphere with Tanzu on an existing cluster.

Provider VDCs backed by a Supervisor Cluster appear with a Kubernetes icon next to their name in the grid that lists all provider VDCs.

4 (Optional) VMware Cloud Director generates automatically a default provider VDC Kubernetes policy for provider VDCs backed by a Supervisor Cluster. You can create additional provider VDC Kubernetes policies for Tanzu Kubernetes clusters. See Create a Provider VDC Kubernetes Policy in Your VMware Cloud Director.

5 Publish a Provider VDC Kubernetes Policy to an Organization VDC in VMware Cloud Director from the **Provider VDCs** tab or Add an Organization VDC Kubernetes Policy in VMware Cloud Director from the **Organization VDCs** tab.

6 Publish the Kubernetes Container Clusters plug-in to service providers. See Publish or Unpublish a Plug-in from a VMware Cloud Director Organization. If you want to enable tenants to create Kubernetes clusters, you must publish the Kubernetes Container Clusters plug-in to those organizations. For more information about managing VMware Cloud Director plug-ins, see Managing VMware Cloud Director Plug-Ins.

7 If you want to grant tenants the rights to create and manage Tanzu Kubernetes clusters, you must publish the **vmware:tkgcluster Entitlement** rights bundle to any organizations that you want to work with clusters. After sharing the rights bundle, you must add the **Edit: Tanzu Kubernetes Guest Cluster** right to the roles you want to create and modify Tanzu Kubernetes clusters. If you want the users also to delete clusters, you must add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the roles. In addition, you can assign the administrator

rights to users that you want to view all Tanzu Kubernetes clusters in an organization or users that you want to manage clusters across sites. For information about the rights and access levels for Runtime Defined Entities (RDEs), see Chapter 14 Managing Defined Entities in VMware Cloud Director.

8 Grant access to tenants or system administrators by creating Access Control List (ACL) entries. For more information on sharing Runtime Defined Entities (RDEs), see Sharing Defined Entities in VMware Cloud Director.

9 Create a Tanzu Kubernetes Cluster in the VMware Cloud Director Service Provider Admin Portal

Add an Organization VDC Kubernetes Policy in VMware Cloud Director

In VMware Cloud Director, you can add an organization VDC Kubernetes policy by using a provider VDC Kubernetes policy. Tenants can use the organization VDC Kubernetes policy to create Tanzu Kubernetes clusters.

When you add or publish a provider VDC Kubernetes policy to an organization VDC, you make the policy available to tenants. The tenants can use the available organization VDC Kubernetes policies to leverage the Kubernetes capacity while creating Tanzu Kubernetes clusters. A Kubernetes policy encapsulates placement, infrastructure quality, and persistent volume storage classes. Kubernetes policies can have different compute limits.

You can add multiple organization VDC Kubernetes policies to a single organization VDC. You can use a single provider VDC Kubernetes policy to create multiple organization VDC Kubernetes policies. You can use the organization VDC Kubernetes policies as an indicator of the service quality. For example, you can publish a Gold Kubernetes policy that allows a selection of the guaranteed machine classes and a fast storage class or a Silver Kubernetes policy that allows a selection of the best effort machine classes and a slow storage class.

Prerequisites

- Verify that you have at least one flex organization VDC in your environment. See Create an Organization Virtual Data Center in VMware Cloud Director.
- Verify that your environment has at least one provider VDC backed by a Supervisor Cluster. The provider VDCs backed by a Supervisor Cluster are marked with a Kubernetes icon on the **Provider VDCs** tab. For more information on vSphere with Tanzu in VMware Cloud Director, see Using Kubernetes with Your VMware Cloud Director.
- Familiarize yourself with the virtual machine class types for Tanzu Kubernetes clusters. See the *vSphere with Kubernetes Configuration and Management* guide in the vSphere documentation.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Organization VDCs**, and click the name of a flex organization VDC.

3 Under Policies, select **Kubernetes**, and click **Add**.

   The **Publish to Organization VDC** wizard appears.

4 Enter a tenant-visible name and description for the organization VDC Kubernetes policy and click **Next**.

5 Select the provider VDC Kubernetes policy that you want to use and click **Next**.

6 Select CPU and Memory limits for the Tanzu Kubernetes clusters created under this policy.

   The maximum limits depend on the CPU and Memory allocations of the organization VDC. When you add the policy, the selected limits act as maximums for the tenants.

7 Choose whether you want to reserve CPU and memory for the Tanzu Kubernetes cluster nodes created in this policy and click **Next**.

   There are two editions for each class type: guaranteed and best effort. A guaranteed class edition fully reserves its configured resources, while a best effort edition allows resources to be overcommitted. Depending on your selection, on the next page of the wizard, you can select between VM class types of the guaranteed or best effort edition.

   - Select **Yes** for VM class types of the guaranteed edition for full CPU and Memory reservations.
   - Select **No** for VM class types of the best effort edition with no CPU and memory reservations.

8 On the **Machine classes** page of the wizard, select one or more VM class types available for this policy.

   The selected machine classes are the only class types available to tenants when you add the policy to the organization VDC.

9 Select one or more storage policies.

10 Review your choices and click **Publish**.

Results

The information about the published policy appears in the list of Kubernetes policies. The published policy creates a Supervisor Namespace on the Supervisor Cluster with the specified resource limits from the policy.

The tenants can start using the Kubernetes policy to create Tanzu Kubernetes clusters. VMware Cloud Director places each Tanzu Kubernetes cluster created under this Kubernetes policy in the same Supervisor Namespace. The policy resource limits become resource limits for the Supervisor Namespace. All tenant-created Tanzu Kubernetes clusters in the Supervisor Namespace compete for the resources within these limits.

What to do next

Manage Quotas on the Resource Consumption of an Organization in VMware Cloud Director

Edit an Organization VDC Kubernetes Policy in VMware Cloud Director

By using VMware Cloud Director Service Provider Admin Portal, you can modify an organization VDC Kubernetes policy to change its description and the CPU and memory limits.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Organization VDCs**, and click the name of a flex organization VDC.
3. Under Policies, select **Kubernetes**, select the policy you want to edit and click **Edit**.

   The **Edit VDC Kubernetes Policy** wizard appears.
4. Edit the description of the organization VDC Kubernetes policy and click **Next**.

   The name of the policy is linked to the Supervisor Namespace, created during the publishing of the policy, and you cannot change it.
5. Edit the CPU and Memory limit for the organization VDC Kubernetes policy and click **Next**.

   You cannot edit the CPU and Memory reservation.
6. Review the new policy details and click **Save**.

Create a Tanzu Kubernetes Cluster in the VMware Cloud Director Service Provider Admin Portal

You can create Tanzu Kubernetes clusters by using the Kubernetes Container Clusters plug-in.

For more information about the different Kubernetes runtime options for the cluster creation, see Using Kubernetes with Your VMware Cloud Director.

You can manage Kubernetes clusters also by using the VMware Cloud Director Container Service Extension CLI. See the VMware Cloud Director Container Service Extension documentation.

VMware Cloud Director provisions Tanzu Kubernetes clusters with the PodSecurityPolicy Admission Controller enabled. You must create a pod security policy to deploy workloads. For information about implementing the use of pod security policies in Kubernetes, see the *Using Pod Security Policies with Tanzu Kubernetes Clusters* topic in the *vSphere with Kubernetes Configuration and Management* guide.

Prerequisites

- Publish the Kubernetes Container Clusters plug-in to any organizations that you want to manage Tanzu Kubernetes clusters.
- Verify that you have at least one organization VDC Kubernetes policy in your organization VDC. To add an organization VDC Kubernetes policy, see Add an Organization VDC Kubernetes Policy in VMware Cloud Director.

- You must publish the **vmware:tkgcluster Entitlement** rights bundle to any organizations that you want to work with clusters. After sharing the rights bundle, you must add the **Edit: Tanzu Kubernetes Guest Cluster** right to the roles you want to create and modify Tanzu Kubernetes clusters. If you want the users also to delete clusters, you must add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the roles. In addition, you can assign the administrator rights to users that you want to view all Tanzu Kubernetes clusters in an organization or users that you want to manage clusters across sites. For information about the rights and access levels for Runtime Defined Entities (RDEs), see Chapter 14 Managing Defined Entities in VMware Cloud Director.
- Grant access to tenants or system administrators by creating Access Control List (ACL) entries. For more information on sharing Runtime Defined Entities (RDEs), see Sharing Defined Entities in VMware Cloud Director.

Procedure

1 From the top navigation bar, select **More > Kubernetes Container Clusters**.

2 (Optional) If the organization VDC is enabled for TKGI cluster creation, on the **Kubernetes Container Clusters** page, select the **vSphere with Tanzu & Native** tab.

3 Click **New**.

4 Select the **vSphere with Tanzu** runtime option and click **Next**.

5 Enter a name for the new Kubernetes cluster and click **Next**.

6 Select the organization VDC to which you want to deploy a Tanzu Kubernetes cluster and click **Next**.

7 Select an organization VDC Kubernetes policy and a Kubernetes version, and click **Next**.

   VMware Cloud Director displays a default set of Kubernetes versions that are not tied to any organization VDC or Kubernetes policy. These versions are a global setting. To change the list of available versions, use the cell management tool to run the `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v` *`version_numbers`* command with comma-separated version numbers.

8 Select the number of control plane and worker nodes in the new cluster.

9 Select machine classes for the control plane and worker nodes, and click **Next**.

10 Select a Kubernetes policy storage class for the control plane and worker nodes, and click **Next**.

11 (Optional) Specify a range of IP addresses for Kubernetes services and a range for Kubernetes pods, and click **Next**.

   Classless Inter-Domain Routing (CIDR) is a method for IP routing and IP address allocation.

Option	Description
`Pods CIDR`	Specifies a range of IP addresses to use for Kubernetes pods. The default value is 192.168.0.0/16. The pods subnet size must be equal to or larger than /24. This value must not overlap with the Supervisor Cluster settings. You can enter one IP range.
`Services CIDR`	Specifies a range of IP addresses to use for Kubernetes services. The default value is 10.96.0.0/12. This value must not overlap with the Supervisor Cluster settings. You can enter one IP range.

12 Review the cluster settings and click **Finish**.

What to do next

- Resize the Kubernetes cluster if you want to change the number of worker nodes.
- Download the kubeconfig file. The kubectl command-line tool uses kubeconfig files to obtain information about clusters, users, namespaces, and authentication mechanisms.
- Delete a Kubernetes cluster.

Upgrade a Tanzu Kubernetes Grid Service Cluster in Your VMware Cloud Director Service Provider Admin Portal

You can upgrade Tanzu Kubernetes Grid Service clusters by using the Kubernetes Container Clusters plug-in.

For more information about the VMware Cloud Director Container Service Extension, see the VMware Cloud Director Container Service Extension Documentation.

For Tanzu Kubernetes Grid Service clusters, if the parent supervisor cluster supports a later Kubernetes version, you can upgrade a Tanzu Kubernetes Grid Service cluster in VMware Cloud Director by using the Kubernetes Container Clusters plug-in.

Procedure

1 From the top navigation bar, select **More > Kubernetes Container Clusters**.

2 Click the radio button next to a Tanzu Kubernetes Grid Service cluster you want to upgrade.

The upgrade column refreshes with information about the availability of an upgrade for the cluster. You can upgrade clusters with status `Available`.

3 Select the Kubernetes version to which you want to upgrade the cluster.

4 Click **Upgrade**.

Understanding Trusted Platform Module Devices in VMware Cloud Director

Starting with VMware Cloud Director 10.4.2, you can create, copy, and edit VMs and vApps with Trusted Platform Module (TPM) devices. A TPM is a software-based representation of a physical Trusted Platform Module 2.0 chip. A TPM acts as any other virtual device.

TPMs provide hardware-based, security-related functions such as random number generation, attestation, key generation, and more. When you add a TPM to a VM, the TPM enables the guest operating system to create and store private keys. The guest operating system cannot access these keys, which reduces the VM attack surface. Usually, compromising the guest operating system compromises its secrets, but enabling a TPM greatly reduces this risk. Only the guest operating system can use these keys for encryption or signing. With an attached TPM, a client can remotely attest the identity of the VM, and verify the software that it is running.

A TPM does not require a physical Trusted Platform Module 2.0 chip to be present on the ESXi host. From the perspective of the VM, a TPM is a virtual device. You can add a TPM to either a new or an existing VM. To secure vital TPM data, a TPM depends on the VM encryption, and you must configure a key provider. When you configure a TPM, the VM files are encrypted but not the disks.

For tenant-relevant information, see Working with Virtual Machines.

To add a TPM device to a VM, your vSphere environment must meet certain requirements.

- Virtual machine requirements
  - EFI firmware
  - VM hardware version 14 and later
- Component requirements
  - vCenter Server 6.7 and later for Windows VMs vCenter Server 7.0 Update 2 and later for Linux VMs
  - Native, standard, or trusted key provider configured for vCenter Server. See the Configuring and Managing a Standard Key Provider, Configuring and Managing vSphere Native Key Provider, or Trusted Infrastructure Overview chapters in the *VMware vSphere Security* documentation.
- Guest OS support
  - Linux
  - Windows Server 2008 and later
  - Windows 7 and later

To perform certain operations for VMs with TPM across vCenter Server instances, you must verify that your environment meets certain prerequisites. The operations are:

- Copy a VM

- Move a VM
- Copy a vApp
- Move a vApp
- Instantiate a vApp template when the template copies the TPM during instantiation.
- Save a vApp as a vApp template to a catalog
- Add a standalone VM to a catalog
- Create a vApp template from an OVF file
- Import a VM from vCenter Server

To perform the operations across vCenter Server instances, your environment must meet the following criteria:

- The key provider used to encrypt each VM must be registered on the target vCenter Server instance under the same name.
- The VM and the target vCenter Server instance are on the same shared storage. Alternatively, fast cross vCenter Server vApp instantiation must be activated. See the fast cross vCenter Server vApp instantiation information in the VMware Cloud Director 10.4 Release Notes.

For VMs with a TPM device, when the target catalog uses any available storage in an organization which has multiple backing vCenter Server instances, VMware Cloud Director does not support the following operations:

- Save a vApp as a vApp template to a catalog
- Add a standalone VM to a catalog
- Create a vApp template from an OVF file
- Importing a VM from vCenter Server as a template

If the target vCenter Server instance is version 8.0 or later, you can replace the TPM device of a VM during the following operations:

- Copy a VM
- Copy a vApp
- Compose a vApp

Table 8-3. TPM Device Options Depending on the vCenter Server Version

Operation	vCenter Server 7.x	vCenter Server 8.x
Create a Standalone Virtual Machine	New TPM device	New TPM device
Create a Virtual Machine from a Template	Copy and replace Depends on the specific VM template.	Copy and replace Depends on the specific VM template.

Table 8-3. TPM Device Options Depending on the vCenter Server Version (continued)

Operation	vCenter Server 7.x	vCenter Server 8.x
Build a New vApp	Copy and replace Depends on the specific VM templates.	Copy and replace Depends on the specific VM templates.
Create a vApp From an OVF Package	New TPM device Uploading an OVF with a TPM RASD section attaches a new TPM device to each VM with a defined TPM.	New TPM device Uploading an OVF with a TPM RASD section attaches a new TPM device to each VM with a defined TPM.
Create a vApp from a vApp Template	Copy and replace Depends on the vApp template.	Copy and replace Depends on the vApp template.
Import a Virtual Machine from vCenter Server as a vApp	Copy	Copy
Add a Virtual Machine to a vApp	New TPM device	New TPM device
Add a VM from a Template to a vApp	Copy and replace Depends on the specific VM template.	Copy and replace Depends on the specific VM template.
Copy a Virtual Machine to a Different vApp	Copy	Copy and replace
Move a Virtual Machine to a Different vApp	Copy	Copy
Copy a Stopped vApp to Another VDC Copy a Powered-On vApp	Copy Applies to all TPM devices within the vApp.	Copy and replace Applies to all TPM devices within the vApp.
Save a vApp as a vApp Template to a Catalog	Copy and replace	Copy and replace
Create a vApp Template from an OVF File	New TPM device Uploading an OVF with a TPM RASD section attaches a new TPM device to each VM with a defined TPM.	New TPM device Uploading an OVF with a TPM RASD section attaches a new TPM device to each VM with a defined TPM.

If you do not specify whether to copy or replace a TPM device in the API, VMware Cloud Director copies the TPM by default. When performing operations on vApps in the UI, the option to copy or replace TPM applies to all VMs within the vApp.

When instantiating a VM from a vApp template containing a TPM device there are some considerations you must take into account.

- If the template was created by using VMware Cloud Director, the instantiation copies or replaces the TPM device based on the selected **TPM Provisioning** option when the template was captured.
- If the template was created by uploading an OVF or OVA, the instantiation replaces the TPM device.

- If the template was created by importing a VM from vCenter Server, the instantiation copies the TPM device.
- If the target vCenter Server meets the TPM requirements, you can perform instantiations across vCenter Server instances for templates for which VMware Cloud Director replaces the TPM devices during instantiation.

When using the VMware Cloud Director API, VMware Cloud Director supports the `moveVApp` API for VMs with a TPM device if the target vCenter Server instance contains the key provider associated with the VM. There is no shared storage requirement for the `moveVApp` API. There are shared storage requirements for other operations that involve moving a vApp.

Importing a VM containing a TPM device from a vCenter Server instance as a vApp preserves the TPM device for the `copy` and `move` operations.

For TPM prerequisites for vCenter Server, see the prerequisite sections in Create a Virtual Machine with a Virtual Trusted Platform Module or Add Virtual Trusted Platform Module to an Existing Virtual Machine in the *vSphere Security* guide.

Create an Organization Virtual Data Center in VMware Cloud Director

To allocate resources to an organization, you must create an organization virtual data center (VDC) in VMware Cloud Director. An organization VDC obtains its resources from a provider VDC. One organization can have multiple organization VDCs.

Prerequisites

Create a provider VDC. See Create a Provider Virtual Data Center in Your VMware Cloud Director.

If you are using VMware Cloud Director 10.5.1 and you want to create an organization VDC that uses NSX tenancy, verify that you activated NSX tenancy for the organization in which you are creating the VDC. See Managing NSX Tenancy in VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**, and click **New**.
3. Enter a name and, optionally, a description for the new organization VDC.
4. (Optional) To deactivate the new organization VDC upon creation, turn off the **Enable the organization VDC** toggle.

   Users cannot deploy vApps on a deactivated organization VDC.
5. Click **Next**.

6 Select the radio button next to the name of the organization to which you want to add this VDC, and click **Next**.

7 Select the radio button next to the name of the provider VDC from which you want the organization VDC to obtain compute and storage resources, and click **Next**.

The provider VDC list displays all activated provider VDC at the site with information about the available resources. The networks list displays information about the networks available to the selected provider VDC.

8 Select an allocation model for this organization VDC, and click **Next**.

Option	Description
Allocation Pool	A percentage of the resources you allocate from the provider VDC are committed to the organization VDC. You can specify the percentage for both CPU and memory.
Pay-As-You-Go	Resources are committed only when users create vApps in the organization VDC.
Reservation Pool	All the resources you allocate are immediately committed to the organization VDC.
Flex	You can control the resource consumption at both the VDC and the individual virtual machine levels. The flex allocation model supports the capabilities of organization VDC compute policies. Flex allocation model supports all allocation configurations that are available in the other allocation models.

9 Configure the allocation settings for the allocation model that you selected, and click **Next**.

Option	Description	Allocation model
Elasticity	Activate or deactivate the elastic pool feature. An elastic organization VDC spans and uses all resource pools associated with its provider VDC.	Flex
Include VM Memory Overhead	Include or exclude memory overhead.	Flex
CPU allocation	The maximum amount of CPU that you want to allocate to the virtual machines running in this organization VDC.	■ Allocation Pool ■ Reservation Pool ■ Flex
Allow CPU resources to grow beyond	To provide unlimited CPU resources to this organization VDC, turn on this toggle.	Reservation Pool
CPU Quota	The maximum amount of CPU consumption for this organization VDC.	■ Pay-as-you-go ■ Flex

Option	Description	Allocation model
CPU resources guaranteed	The percentage of CPU resources that you want to guarantee to a virtual machine running in this organization VDC. You can control overcommitment of CPU resources by guaranteeing less than 100 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the CPU allocation is committed for this organization VDC.	■ Allocation Pool ■ Pay-as-you-go ■ Flex
vCPU Speed	The vCPU speed. Virtual machines running in the organization VDC are assigned this amount of GHz per vCPU.	■ Pay-as-you-go ■ Flex
Memory allocation	The maximum amount of memory that you want to allocate to the virtual machines running in the organization VDC.	■ Allocation Pool ■ Reservation Pool
Memory Quota	The maximum amount of memory consumption for this organization VDC.	■ Pay-as-you-go ■ Flex
Memory resources guaranteed	The percentage of memory resources that you want to guarantee to virtual machines running in the organization VDC. You can overcommit resources by guaranteeing less than 100 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the memory allocation is committed for this organization VDC.	■ Allocation Pool ■ Pay-as-you-go ■ Flex
Maximum number of VMs	The maximum number of virtual machines that can exist in the organization VDC.	■ Allocation Pool ■ Pay-as-you-go ■ Reservation Pool ■ Flex

10 Configure the storage settings for this organization VDC, and click **Next**.

The list contains the activated storage policies on the source provider VDC.

a Select the check boxes of one or more storage policies that you want to add to this organization VDC.

b (Optional) To limit the amount of the allocated storage capacity for a selected storage policy, select **Limited** from the drop-down menu in the **Allocation Type** cell, and enter the maximum capacity in the **Allocated Storage** cell.

c (Optional) To change the default storage policy, from the **Default instantiation policy** drop-down menu, select the target default storage policy.

VMware Cloud Director uses the default storage policy for all virtual machine provisioning operations where the storage policy is not specified at the virtual machine or vApp template level.

d (Optional) To activate thin provisioning for virtual machines in the organization VDC, turn on the **Thin provisioning** toggle.

e (Optional) To deactivate fast provisioning for virtual machines in the organization VDC, turn off the **Fast provisioning** toggle.

11 (Optional) If you are using VMware Cloud Director 10.5.1, toggle on the **Networking Tenancy** option to activate NSX tenancy for the organization VDC.

   Note that you cannot change this setting later.

12 If you are not using NSX tenancy, configure the network pool settings for this organization VDC, and click **Next**.

   VMware Cloud Director uses the network pool to create vApp networks and internal organization VDC networks.

   - To skip adding a network pool at this stage, turn off the **Use Network Pool** toggle.
   - To configure a network pool, select the radio button next to the name of the target network pool, and enter the Quota for this organization VDC.

     The quota is the maximum number of provisioned networks in the organization VDC backed by this network pool. Must not exceed the number of the available networks for the selected network pool.

13 Review the **Ready to Complete** page, and click **Finish**.

Activate or Deactivate an Organization Virtual Data Center in VMware Cloud Director

To prevent additional vApps and virtual machines from using compute and storage resources from an organization virtual data center, in VMware Cloud Director Service Provider Admin Portal, you can deactivate this organization virtual data center. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Select the radio button next to the name of the target organization virtual data center, and click **Enable** or **Disable**.

4 To confirm, click **OK**.

Delete an Organization Virtual Data Center From VMware Cloud Director

To remove all resources of an organization virtual data center from an organization, you can delete this organization virtual data center by using the VMware Cloud Director Service Provider Admin Portal. The resources remain unaffected in the source provider virtual data center.

Important This operation permanently removes the organization virtual data center and all its VMs, vApps, organization virtual data center networks, and edge gateways.

Prerequisites

If you want to keep certain VMs, vApps, vApp templates, or media files that belong to the target organization virtual data center, move them to another organization virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Select the radio button next to the name of the organization virtual data center that you want to remove, and click **Delete**.

4 If this organization virtual data center contains any resources, such as VMs, vApps, organization virtual data center networks, and edge gateways, to confirm their removal, select the check box for each resource type.

5 To confirm, click **Delete**.

Modify the Name and the Description of an Organization Virtual Data Center in VMware Cloud Director

As your VMware Cloud Director installation expands, you might want to assign a more meaningful name or description to an existing organization virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 On the **General** tab, in the upper-right corner, click **Edit**.

4 Enter a new name and description, and click **Save**.

Modify the Allocation Model Settings of an Organization Virtual Data Center in VMware Cloud Director

Using the VMware Cloud Director Service Provider Admin Portal, you cannot change the allocation model for an organization virtual data center (VDC), but you can change the allocation settings for the allocation model that you specified during the creation of the organization VDC.

Note By using the VMware Cloud Director API, you can convert the allocation model of any organization VDC. Alternatively, using the Service Provider Admin Portal, you can convert the non-Flex VDC into a Flex VDC by publishing an incompatible compute policy to the VDC.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 On the **Allocation** tab, in the upper-right corner, click **Edit**.

4 Edit the allocation model settings, and click **Save**.

Modifying the Storage Settings of an Organization Virtual Data Center in VMware Cloud Director

By using the VMware Cloud Director Service Provider Admin Portal, you can modify the storage settings that you configured during the creation of the organization virtual data center.

You can view the list of the storage containers associated with a storage policy by navigating to the **Infrastructure Resources** tab, in the left panel, selecting **Storage Policies**, and clicking the name of the storage policy you want to view.

Enabling VM Encryption on VMware Cloud Director Storage Policies of an Organization VDC

In VMware Cloud Director, you can add an encryption-enabled storage policy to an organization VDC. You can encrypt VMs and disks by associating a VM or disk with a storage policy that has the VM Encryption capability.

You can improve the security of your data by using VM encryption. Encryption protects not only your virtual machine but also virtual machine disks and other files. You can view the capabilities of storage policies and the encryption status of VMs and disks in the API and UI. You can perform all operations on encrypted VMs and disks that are supported in the respective vCenter Server version.

If the provider VDC has a storage policy with enabled VM Encryption, you can add the encryption-enabled policy to an organization VDC. See Enabling VM Encryption on Storage Policies of a Provider Virtual Data Center in Your VMware Cloud Director and Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center. After that, by using the VMware Cloud Director Tenant Portal, tenants can associate a VM or disk with a storage policy with enabled VM Encryption.

VM Encryption Limitations

The following actions are not supported.

- Encrypt or decrypt a powered-on VM or its disks.
- Export an OVF of an encrypted VM.
- Encrypt and decrypt the disks of a VM with a snapshot if the disks are part of the snapshot.
- Decrypt a VM when its disk is on an encrypted policy.
- Add an encrypted disk to a non-encrypted VM.
- Encrypt an existing disk on a non-encrypted VM.
- Add an encrypted named disk to unencrypted VM.
- Create an encrypted linked clone.
- Encrypt a linked clone VM or its disks.
- Instantiate, move, or clone VMs across vCenter Server instances when the source VM is encrypted.

Note On a fast-provisioned organization VDC, if the source or target VM is encrypted and you want to create a clone, VMware Cloud Director always creates a full clone.

Identifying a VM Encryption Storage Capability

By default, **System administrators** and **Organization administrators** have the necessary rights to view the organization VDC storage capabilities and whether VMs and disks are encrypted. **vApp Authors** can view the encryption status of VMs and disks. For more information about roles and rights, see Predefined VMware Cloud Director Roles and Their Rights.

You can view all storage capabilities in the **Capabilities** column under **Resources > vSphere Resources > Storage Policies**. This column displays the VM encryption, tag-based association, vSAN , and IOPS limiting storage capabilities. To view the full list of storage capabilities, expand the row by clicking the arrow on the left side of the storage policy name.

You can also view the storage capability information in the **Storage** tab of an organization VDC.

Modify the VM Provisioning Settings of a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can modify the virtual machine thin provisioning and fast provisioning settings that you configured during the creation of the organization virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** and click **Edit**.

4 (Optional) Modify the thin provisioning setting.

- To deactivate thin provisioning for virtual machines in the organization virtual data center, turn off the **Thin provisioning** toggle.
- To activate thin provisioning for virtual machines in the organization virtual data center, turn on the **Thin provisioning** toggle.

5 (Optional) Modify the fast provisioning setting.

- To activate fast provisioning for virtual machines in the organization virtual data center, turn on the **Fast provisioning** toggle.
- To deactivate fast provisioning for virtual machines in the organization virtual data center, turn off the **Fast provisioning** toggle.

6 Click **Edit**.

Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can configure an organization virtual data center to support a VM storage policy that you previously added to the backing provider virtual data center.

Prerequisites

You added the target VM storage policy to the source provider virtual data center. See Add a VM Storage Policy to a Provider Virtual Data Center in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** , and click **Add**.

   You can see a list of the available additional storage policies in the source provider virtual data center.

4 Select the check boxes of one or more storage policies that you want to add, and click **Add**.

Change the Default Storage Policy on a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can change the default storage policy that you configured during the creation of an organization virtual data center.

VMware Cloud Director uses the default storage policy for all virtual machine provisioning operations where the storage policy is not specified at the virtual machine or vApp template level.

Prerequisites

- The target default storage policy is added to the organization virtual data center. See Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center.
- The target default storage policy is enabled on the organization virtual data center. See Activate or Deactivate a Storage Policy on a VMware Cloud Director Organization Virtual Data Center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target default storage policy, and click **Set as default**.

5 To confirm, click **OK**.

Edit the Limit of a Storage Policy on a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can change the limit of the allocated storage capacity that you configured for a storage policy during the creation of an organization virtual data center.

You can set the allocated storage capacity as unlimited or configure a maximum amount of allocated storage capacity for a storage policy on an organization virtual data center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target storage policy, and click **Edit limit**.

5 Configure the limit setting for this storage policy.

   - To set a limit, select the upper radio button, and enter the maximum amount of storage resource for this storage policy on this organization virtual data center.

   - To set no limit, select the **Unlimited** radio button.

6 Click **Edit**.

Modify the Metadata for a VM Storage Policy on a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can add, edit, and delete metadata for a storage policy on an organization virtual data center.

By using object metadata, you can associate user-defined `name=value` pairs with a storage policy on an organization virtual data center. You can use object metadata in vCloud API query filter expressions.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target storage policy, and click **Metadata**.

5 Click **Edit**.

6 (Optional) To add a key-value pair, click **Add**, enter a name and a value, and select a type for the new key-value pair.

7 (Optional) To edit a key-value pair, enter a new name and a value, and select a new type for the key-value pair.

8 (Optional) To remove a key-value pair, in the right end of the row, click the **Delete** icon.

9 Click **Save**, and click **OK**.

Activate or Deactivate a Storage Policy on a VMware Cloud Director Organization Virtual Data Center

To prevent additional vApps and virtual machines from using a storage policy on a VMware Cloud Director organization virtual data center, you can deactivate this storage policy on the organization virtual data center. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines on this storage policy.

You cannot deactivate the default storage policy.

Prerequisites

If you want to deactivate the default storage policy, Change the Default Storage Policy on a VMware Cloud Director Organization Virtual Data Center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target storage policy, and click **Enable** or **Disable**.

5 To confirm, click **OK**.

Delete a Storage Policy from a VMware Cloud Director Organization Virtual Data Center

To prevent a VMware Cloud Director organization virtual data center from using a storage policy, you can remove this storage policy from the organization virtual data center. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines on this storage policy.

Prerequisites

Deactivate the storage policy that you want to remove. See Activate or Deactivate a Storage Policy on a VMware Cloud Director Organization Virtual Data Center.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target storage policy, and click **Remove**.

5 To confirm, click **Remove**.

Edit the VMware Cloud Director Organization VDC Storage Policy Settings

In VMware Cloud Director, you can change the I/O operations per second (IOPS) settings of an organization VDC storage policy. By default, the organization VDC storage policies inherit the provider VDC storage policy settings. You can customize the settings per organization VDC storage policy.

Prerequisites

Add a VM Storage Policy to a VMware Cloud Director Organization Virtual Data Center

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the target storage policy, and click **Edit Settings**.

5 If you want the IOPS settings of the organization VDC storage policy to be different from the provider VDC storage policy, turn off the **Inherit From Provider VDC** toggle.

6 If you want to limit the I/O operations per second, turn on the **IOPS Limiting Enabled** toggle.

7 If you want IOPS to be considered during placement, turn on the **Impact Placement** toggle.

   If the **Impact Placement** toggle is turned on, VMware Cloud Director provides IOPS load balancing across datastores. When you set IOPS settings for a disk, VMware Cloud Director considers datastores with enough IOPS capacity for the selected disk. If the **Impact Placement** toggle is turned off, you do not need to set IOPS capacities per datastore and you can use Storage DRS clusters.

8 (Optional) Configure the maximum and default IOPS settings.

9 Click **Save**.

Migrate Storage Policy Entities Using the VMware Cloud Director Service Provider Admin Portal

Starting with VMware Cloud Director 10.5.1, if you want to merge two storage policies or to reassign storage entities in bulk before removing a storage policy, you can migrate one or more storage policy entities from one policy to another.

Prerequisites

Verify that there are at least two storage policies in the organization VDC.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Policies**, select **Storage** .

4 Click the radio button next to the name of the target storage policy, and click **Migrate Storage**.

5 Select the type of entities that you want to migrate.

   You can select to migrate named disks, catalog media, and virtual machines (VMs).

6 Select the storage policy to which you want to migrate the entities to.

7 Click **Migrate**.

Results

The assigned storage policy of the entities you selected changes to the target storage policy.

Edit the Network Settings of a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can change the network pool from which new networks are provisioned in an organization virtual data center. You can also enable organization virtual data centers to become eligible for cross-virtual data center networking.

A network pool is a group of undifferentiated networks that you can use to create vApp networks, routed organization VDC networks, and isolated organization VDC networks. You can change the network pool for new networks. Existing networks continue to use the old network pools.

With organization virtual data centers that are enabled for cross-virtual data center networking, organization users with relevant rights can create data center groups and stretched layer 2 networks in these groups.

Starting with VMware Cloud Director 10.3, **system administrators** can assign a VLAN or a port-group backed network pool to an organization VDC, even if their provider VDC is backed by NSX. **Organization administrators** can then create isolated organization VDC networks backed by such network pools.

Prerequisites

- If you want to enable data center group networking with NSX Data Center for vSphere for an organization virtual data center, verify that you configured cross-vCenter NSX on the backing provider virtual data center.
- If you want to use VLAN and port-group backed network pools in an organization VDC that is backed by a provider VDC which uses NSX, you must ensure that the NSX cluster hosts are added to the vSphere distributed switch. See *vSphere Networking*.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Click **Networking**, and on the **Network Pool** tab, in the upper-right corner, click **Edit**.

   You can see the networks used by this organization virtual data center.

4 (Optional) Configure the network pool settings for this organization virtual data center.

   - If you do not want a network pool for this organization virtual data center, turn off the **Specify network pool** toggle.
   - If you want to configure a network pool for this organization virtual data center, follow these steps:

     a Turn on the **Specify network pool** toggle.

       You can see a list of the available network pools with information about their use, available networks, and capacity.

     b Select the radio button next to the name of the target resource pool.

     c Configure the quota for this network pool in this organization virtual data center.

       The quota is the maximum number of provisioned networks. Must not exceed the number of the available networks for the selected network pool.

5 To enable cross-virtual data center networking for this organization virtual data center, turn on the **Cross VDC Networking** toggle.

6 Click **Save**.

Set a Segment Profile Template for a VMware Cloud Director Organization VDC

In VMware Cloud Director, you can set segment profiles templates to be applied to all VDC networks and to all vApp networks within an organization VDC upon their creation.

Prerequisites

- Verify that you created segment profiles in NSX Manager.
- Verify that you Create a Segment Profile Template in VMware Cloud Director to apply.

Procedure

1 From the top navigation bar, select **Resources**, and click the **Cloud Resources** tab.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Under **Networking**, select **Segment Profile Templates** and click **Edit**.

4 From the **Org VDC Networks** drop-down menu, select a custom template to apply to organization VDC networks .

5 From the **vApp Networks** drop-down menu, select a custom template to apply to vApp networks.

6 Click **Save**.

Assign an Edge Cluster to a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, to enable networking services such as NAT and firewall for the routed vApp networks within an organization VDC that is backed by NSX, you must assign an edge cluster to the organization VDC. In NSX, the service edge cluster is where vApp edge gateways are deployed.

Prerequisites

Verify that the organization VDC to which you are assigning an edge cluster is backed by NSX.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.

3 Click the **Network** tab, scroll down to the Edge Cluster pane and click **Edit**.

4 Select an edge cluster to assign to the organization virtual data center.

5 Click **Save**.

Configuring Cross-Virtual Data Center Networking in VMware Cloud Director

The cross-virtual data center networking feature enables organizations that have virtual data centers backed by multiple vCenter Server instances to stretch layer 2 networks across up to four virtual data centers. Cross-virtual data center networking relies on cross-vCenter NSX and can span multiple VMware Cloud Director sites.

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

With cross-virtual data center networking, organizations can group up to four virtual data centers and configure egresses and stretched layer 2 networks in each group.

The participating organization virtual data centers can belong to different VMware Cloud Director sites. See Configuring and Managing Multisite Deployments in Your VMware Cloud Director.

Organizations can use cross-virtual data center networking to implement high availability solutions or distributed systems architectures, where an application can be distributed across multiple virtual data centers or sites.

The **system administrator** must configure the underlying cross-vCenter NSX environment, the VMware Cloud Director servers, and enable cross-virtual data center networking for each virtual data center.

1 Configure one of the NSX-V Manager instances as a Primary NSX-V Manager instance. See the *Cross-vCenter NSX Installation Guide*.

   a Deploy the NSX cluster on the primary NSX-V Manager instance.

   b Prepare the ESXi hosts on the primary NSX-V Manager instance.

   c Configure VXLAN from the primary NSX-V Manager instance.

   d Assign the primary role to the NSX-V Manager instance.

   e Create a pool for segment IP for the universal transport zone.

   f Add a universal transport zone.

2 Configure the rest of the NSX-V Manager instances as Secondary NSX Managers. See the *Cross-vCenter NSX Installation Guide*.

   a Prepare the ESXi hosts on each secondary NSX Manager instance.

   b Configure VXLAN from each secondary NSX-V Manager instance.

   c Assign the secondary role to each NSX-V Manager instance.

   d Connect the ESXi clusters to the universal transport zone.

3 Configure the control VM properties for each NSX-V Manager instance. See Modify NSX Manager Settings in Your VMware Cloud Director.

4 Create a VXLAN backed network pool using a universal type transport zone from any vCenter Server instance. See Create a Network Pool Backed by an NSX Data Center for vSphere Transport Zone in Your VMware Cloud Director.

   Note For multisite deployments, you must create a VXLAN backed network pool in each VMware Cloud Director site.

5 Enable cross-virtual data center networking on each organization virtual data center. See Edit the Network Settings of a VMware Cloud Director Organization Virtual Data Center.

6 If the organization has multisite virtual data centers, verify that the installation IDs in the different VMware Cloud Director sites are different. If there are VMware Cloud Director sites that are configured with the same installation ID, see Regenerating MAC Addresses for Multisite Stretched Networks in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

The **organization administrator** can now create and configure data center groups, egresses, and stretched networks. For information about managing cross-virtual data center networking, see the *VMware Cloud Director Tenant Guide*.

Modify the Metadata for a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can add, edit, and delete metadata for an organization virtual data center.

By using object metadata, you can associate user-defined `name=value` pairs with an organization virtual data center. You can use object metadata in vCloud API query filter expressions.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.
3. Click the **Metadata** tab.
4. Click **Edit**.
5. (Optional) To add a key-value pair, click **Add**, enter a name and a value, and select a type for the new key-value pair.
6. (Optional) To edit a key-value pair, enter a new name and a value, and select a new type for the key-value pair.
7. (Optional) To remove a key-value pair, in the right end of the row, click the **Delete** icon.
8. Click **Save**, and click **OK**.

View the Resource Pools of a VMware Cloud Director Organization Virtual Data Center

In VMware Cloud Director, you can view a list of the vCenter Server resource pools that an organization virtual data center uses.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**, and click the name of the target organization virtual data center.
3. Click the **Resource Pools** tab.

Results

You can see a table with the resource pools in use by the organization virtual data center, and the vCenter Server instance to which each resource pool belongs.

Managing the Distributed Firewall on a VMware Cloud Director Organization Virtual Data Center

To provide Layer 3 and Layer 2 network security in a VMware Cloud Director organization virtual data center, you can enable and create rules for the distributed firewall on this organization virtual data center. With the distributed firewall rules, you can protect traffic traveling between virtual machines in an organization virtual data center.

VMware Cloud Director supports distributed firewall services on organization virtual data centers that are backed by NSX Data Center for vSphere.

For creating the distributed firewall rules, you can use various grouping objects and security groups. See Custom Grouping Objects for NSX Data Center for vSphere Edge Gateways in the VMware Cloud Director Service Provider Admin Portal and Working with Security Groups for NSX Data Center for vSphere Edge Gateways by Using Your VMware Cloud Director Service Provider Admin Portal.

For information about protecting traffic to and from an edge gateway, see Managing an NSX Data Center for vSphere Edge Gateway Firewall in the VMware Cloud Director Service Provider Admin Portal.

Activate the Distributed Firewall on a VMware Cloud Director Organization Virtual Data Center

Before you can manage the distributed firewall settings on a VMware Cloud Director organization virtual data center, you must activate the distributed firewall on this organization virtual data center.

VMware Cloud Director supports distributed firewall services on organization virtual data centers that are backed by NSX Data Center for vSphere.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 On the **Distributed Firewall > General** tab, turn on the **Enable Distributed firewall** toggle.

Results

You can see the default firewall rules, which allow all Layer 3 and Layer 2 traffic to pass through the organization virtual data center.

- On the **Distributed Firewall > General** tab, you can see the default distributed firewall rule for Layer 3 traffic, named Default Allow Rule.
- On the **Distributed Firewall > Ethernet** tab, you can see the default distributed firewall rule for Layer 2 traffic, named Default Allow Rule.

Add a Distributed Firewall Rule by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 by Using Your VMware Cloud Director Service Provider Admin Portal and View Service Groups Available for Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal.

Prerequisites

- Activate the Distributed Firewall on a VMware Cloud Director Organization Virtual Data Center
- 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 by Using Your VMware Cloud Director Service Provider Admin Portal.
- If you want to use a MAC set as a source or destination in a rule, Create a MAC Set for Use in Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal.
- If you want to use a Security group as a source or destination in a rule, Create a Security Group by Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 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.

5 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.

6 Click in the **Name** cell and type in a name.

7 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. Enter 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

8 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. Enter 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

9 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 Enter 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**.

10 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.

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

12 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**.

13 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.

14 Click **Save Changes**.

Edit a Distributed Firewall Rule by Using Your VMware Cloud Director Service Provider Admin Portal

In a VMware Cloud 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 by Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

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

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

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

   - Edit a rule name by double-clicking in its **Name** cell and enter 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.

5 Click **Save Changes**.

Custom Grouping Objects for NSX Data Center for vSphere Edge Gateways in the VMware Cloud Director Service Provider Admin Portal

The NSX Data Center for vSphere software in your VMware Cloud 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 by Using Your VMware Cloud Director Service Provider Admin Portal

An IP set is a group of IP addresses that you can create at a VMware Cloud Director 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. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

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 To save this IP set, click **Keep**.

Results

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 by Using Your VMware Cloud Director Service Provider Admin Portal

A MAC set is a group of MAC addresses that you can create at an organization virtual data center level in VMware Cloud Director. You can use a MAC set as the source or destination in a firewall rule.

You create a MAC set by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

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 To save the MAC set, click **Keep**.

Results

The new MAC set is available for selection as the source or destination in firewall rules.

View Services Available for Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

2 Click the **Services** tab.

Results

The available services are displayed on the screen.

View Service Groups Available for Firewall Rules by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 by using the **Grouping Objects** page. To open this page, you must navigate either to the distributed firewall settings of the organization VDC, or to the services settings of an edge gateway that belongs to the organization VDC.

Procedure

1 Open the **Grouping Objects** page.

Option	Action
From the distributed firewall settings of the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Organization VDCs**. c Select the radio button next to the name of the target organization virtual data center, and click **Manage firewall**. d Click the **Grouping Objects** tab.
From the services settings of an edge gateway on the organization VDC	a From the top navigation bar, under **Resources**, select **Cloud Resources**. b In the left panel, click **Edge Gateways**. c Select the radio button next to the name of an edge gateway that belongs to the target organization virtual data center, and click **Services**. d Click the **Grouping Objects** tab.

2 Click the **Service Groups** tab.

Results

The available service groups are displayed on the screen. The Description column displays the services that are grouped in each service group.

Working with Security Groups for NSX Data Center for vSphere Edge Gateways by Using Your VMware Cloud Director Service Provider Admin Portal

A security group is a collection of assets or grouping objects in VMware Cloud Director, 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 by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, you can create user-defined security groups.

Prerequisites

If you want to use security tags with security groups, Create and Assign Security Tags by Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2. In the left panel, click **Organization VDCs**.
3. Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.
4. Click the **Grouping Objects > Security Groups** tab.
5. Click the **Create** (+) button.
6. 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.
7. (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**.
8. (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.
9. (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.
10. To preserve your changes, click **Keep**.

Results

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

Edit a Security Group by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, you can edit user-defined security groups.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.
4. Click the **Grouping Objects > Security Groups** tab.
5. Select the security group you want to edit.

   The details for the security group display below the list of security groups.
6. (Optional) Edit the name and the description of the security group.
7. (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**.
8. (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**.
9. (Optional) Delete a dynamic member set by clicking the **Delete** icon next to the member set that you want to delete.

10 (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.

11 (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.

12 Click **Save changes**.

   The changes to the security group are saved.

Delete a Security Group by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, you can delete a user-defined security group.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 Click the **Grouping Objects > Security Groups** tab.

5 Select the security group you want to delete.

6 Click the **Delete** button.

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

Results

The security group is deleted.

Working with Security Tags for NSX Data Center for vSphere Edge Gateways by Using Your VMware Cloud Director Service Provider Admin Portal

Security tags are VMware Cloud Director 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 by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.
4. Click the **Security Tags** tab.
5. Click the **Create** (+) button, and enter a name for the security tag.
6. (Optional) Enter a description for the security tag.

7 (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.

8 When you complete assigning the tag to the selected virtual machines, click **Keep**.

Results

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 by Using Your VMware Cloud Director Service Provider Admin Portal.

Change the Security Tag Assignment by Using Your VMware Cloud Director Service Provider Admin Portal

After you create a security tag, by using the VMware Cloud Director Service Provider Admin Portal, 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 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 Click the **Security Tags** tab.

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

6 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.

7 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.

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

Results

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 by Using Your VMware Cloud Director Service Provider Admin Portal.

View Applied Security Tags by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 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**.

5 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.

Results

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 by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 information are no longer run against the virtual machine.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, click **Organization VDCs**.
3. Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.
4. Click the **Security Tags** tab.
5. From the list of security tags, select the security tag that you want to edit.
6. Click the **Edit** button.
7. Edit the name and the description of the security tag.
8. Assign the tag to or remove the assignment from the virtual machines that you select.
9. 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 for NSX Data Center for vSphere Edge Gateways by Using Your VMware Cloud Director Service Provider Admin Portal

.

Delete a Security Tag by Using Your VMware Cloud Director Service Provider Admin Portal

By using the VMware Cloud Director Service Provider Admin Portal, 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 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, click **Organization VDCs**.

3 Click the radio button next to the target organization virtual data center, and click **Manage Firewall**.

4 Click the **Security Tags** tab.

5 From the list of security tags, select the security tag that you want to delete.

6 Click the **Delete** button.

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

Results

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 for NSX Data Center for vSphere Edge Gateways by Using Your VMware Cloud Director Service Provider Admin Portal.

Managing Dedicated vCenter Server Instances in VMware Cloud Director

9

With dedicated vCenter Server instances, you can use VMware Cloud Director as a central point of management (CPOM) for your vSphere environments.

When you add a vCenter Server instance to VMware Cloud Director, you can specify the purpose of the instance.

Dedicated vCenter Server

The infrastructure of an attached vCenter Server instance is encapsulated as a Software-Defined Data Center (SDDC) and is fully dedicated to a single tenant. You create a dedicated vCenter Server instance by activating the tenant access for that instance. After you activate the tenant access, you can publish a dedicated vCenter Server instance to a tenant.

Shared vCenter Server

The provider can use different resource pools of the vCenter Server instance across multiple provider VDCs and then allocate those resource pools to different tenants. A shared vCenter Server instance cannot be published to tenants.

None

The vCenter Server instance does not have any specific purpose.

VMware Cloud Director can act as an HTTP proxy server for the dedicated vCenter Server instances and the vCenter Server instances that do not have a set purpose.

With dedicated vCenter Server instances, you can use VMware Cloud Director as a central point of management for all your vSphere environments.

- You can dedicate the resources of a vCenter Server instance to a single tenant by publishing the corresponding dedicated vCenter Server only to its organization. The tenant does not share these resources with other tenants. The tenant can access this dedicated vCenter Server instance by using a UI or API proxy without a VPN required.
- You can use VMware Cloud Director as a lightweight directory to register all your vCenter Server instances.
- You can use VMware Cloud Director as an API endpoint for all your vCenter Server instances.

You can activate the tenant access and mark a vCenter Server instance as dedicated, during or after the attachment of the target vCenter Server instance to VMware Cloud Director. See Attach a vCenter Server Instance Alone or Together with an NSX-V Manager Instance to VMware Cloud Director.

With an attached vCenter Server instance, you can create either a shared vCenter Server or a dedicated vCenter Server. If you created a shared vCenter Server instance, you cannot use this vCenter Server instance to create a dedicated vCenter Server, and the reverse.

You can create endpoints that tenants can use to access the underlying vSphere environment. The VMware Cloud Director credentials are for the proxied components that connect to vCenter Server. The vCenter Server instances have different credentials.

Dedicated vCenter Server instances in VMware Cloud Director remove the requirement for vCenter Server to be publicly accessible. To control the access, you can activate and deactivate the tenant access to an SDDC in VMware Cloud Director.

An endpoint is the access point to a component from an SDDC, for example, a vCenter Server instance, an ESXi host, or an NSX-V Manager instance. You can connect an endpoint to a proxy. By activating and deactivating a proxy, you can allow and stop the tenant access through that proxy.

Starting with VMware Cloud Director 10.2, if you use the API to query the dedicated vCenter Server and proxy entities and your tenant configuration supports multisite associations, VMware Cloud Director returns a multisite response. The results are from all available associations.

Creating and Managing Dedicated vCenter Server Instances

To create and manage dedicated vCenter Server instances and proxies, you can use the Service Provider Admin Portal or the VMware Cloud Director OpenAPI. For VMware Cloud Director OpenAPI, see Getting Started with VMware Cloud Director OpenAPI.

Important VMware Cloud Director requires a direct network connection to each dedicated vCenter Server instance. If the vCenter Server instance uses an external Platform Services Controller, VMware Cloud Director requires a direct network connection to the Platform Services Controller as well.

To use VMware OVF Tool in a proxied dedicated vCenter Server, VMware Cloud Director requires a direct connection to each ESXi host.

1 Create a dedicated vCenter Server instance.

   When you add a vCenter Server instance to the VMware Cloud Director environment, you can create a dedicated vCenter Server instance by activating the tenant access in the **Add vCenter Server** wizard. See Add the vCenter Server Instance to VMware Cloud Director.

Creating a dedicated vCenter Server instance also creates a default endpoint for it. While attaching the vCenter Server instance, you can also create a proxy. However, the default endpoint is not connected to any proxy by default. You must edit the default endpoint or create a new one to connect it to a proxy. See Create an Endpoint in VMware Cloud Director.

You can activate the tenant access of vCenter Server instances that are already added to VMware Cloud Director and do not have a specified use. See Enable the Tenant Access of an Attached vCenter Server in VMware Cloud Director. Activating the tenant access makes the vCenter Server instance available to be published to tenants.

2 Add a proxy.

You can create a proxy either when you attach a vCenter Server instance to VMware Cloud Director or later. If the vCenter Server instance uses an external Platform Services Controller, VMware Cloud Director creates a proxy for the Platform Services Controller as well. With parent and child proxies, you can hide certain proxies from the tenants or you can activate and deactivate groups of child proxies through their parent proxies. For information on creating a proxy after you add a vCenter Server instance to VMware Cloud Director, see Add a VMware Cloud Director Proxy for Accessing the Underlying vCenter Server Resources.

You can edit, activate, deactivate, and delete proxies from the **Proxies** tab under **vSphere Resources**.

Note When you add a proxy to a dedicated vCenter Server instance, you must upload the certificate and the thumbprint, so that tenants can retrieve the certificate and the thumbprint if the proxied component uses self-signed certificates.

To view and manage certificates and certificate revocation lists (CRLs), see Manage the Proxy Certificates and CRLs in VMware Cloud Director.

3 Get the certificate and the thumbprint of the created proxies, and verify that the certificate and the thumbprint are present and correct. See Manage the Proxy Certificates and CRLs in VMware Cloud Director.

4 Publish the dedicated vCenter Server instance to one or more organizations.

You can publish a dedicated vCenter Server instance to a tenant and make it visible in the VMware Cloud Director Tenant Portal. In most cases, one vCenter Server instance should be published only to one tenant. See Publish a Dedicated vCenter Server to VMware Cloud Director.

5 To enable the tenants to access the dedicated vCenter Server instances and proxies from the VMware Cloud Director Tenant Portal, you must publish the **CPOM extension** plug-in to their organizations. See Publish or Unpublish a Plug-in from a VMware Cloud Director Organization.

Advanced Central Point of Management Settings

Starting with VMware Cloud Director 10.5, you can activate two advanced settings so that a vCenter Server instance can back both a provider VDC and a dedicated vCenter Server instance and to publish that dedicated vCenter Server instance to tenants. The advanced central point of management settings are deactivated by default. To access these settings, you can use the VMware Cloud Director configurations API endpoint and configuration value key.

Warning Having a vCenter Server that backs both a provider VDC and a dedicated vCenter Server instance exposes the risk of tenancy boundary violations. You must consider thoroughly these settings before you activate them. You can activate them for very specific use cases or for testing and proof of concept purposes.

The two configuration value keys for the advanced settings are as follows:

- `system.setting.allowVcTenantAndProviderScoped` - if activated, the same vCenter Server instance can back both a provider VDC and a dedicated vCenter Server instance. If a vCenter Server instance backs both, the VMware Cloud Director UI shows the `usage` of the instance as `empty`.

  ```
  /opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
  system.setting.allowVcTenantAndProviderScoped -v true_or_false
  ```

- `vcloud.sddc.allowPublishOfProviderScoped` - is activated, you can publish to tenants dedicated vCenter Server instances backed by vCenter Server which is also backing a provider VDC. For publishing a dedicated vCenter Server instance, see Publish a Dedicated vCenter Server to VMware Cloud Director.

  ```
  /opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
  vcloud.sddc.allowPublishOfProviderScoped -v true_or_false
  ```

Read the following topics next:

- Enable the Tenant Access of an Attached vCenter Server in VMware Cloud Director
- Publish a Dedicated vCenter Server to VMware Cloud Director
- Configure Proxy Routing in VMware Cloud Director

Enable the Tenant Access of an Attached vCenter Server in VMware Cloud Director

You can enable the tenant access of vCenter Server instances that are already added to VMware Cloud Director and do not have a specified use. Enabling the tenant access creates a dedicated vCenter Server instance and makes it available to be published to tenants.

With an attached vCenter Server instance, you can create either a shared vCenter Server or a dedicated vCenter Server. If you created a shared vCenter Server instance, and you want to use it as a dedicated vCenter Server, you must first delete all provider virtual data centers (VDCs) that are using the resources of the vCenter Server instance. Deleting all provider VDCs linked to the shared vCenter Server instance changes its status to None.

Prerequisites

Verify that you have in your environment at least one attached vCenter Server that is not dedicated or shared.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.
3. Select a vCenter Server without a specified purpose in the **Usage** column.
4. Click **Enable Tenant Access**.

What to do next

Publish a Dedicated vCenter Server to VMware Cloud Director.

Publish a Dedicated vCenter Server to VMware Cloud Director

You can publish a dedicated vCenter Server to a tenant and make it visible through the VMware Cloud Director Tenant Portal. By default, one vCenter Server should be published only to one tenant.

By default, an SDDC is a vCenter Server instance that you dedicate to a single tenant by publishing the corresponding dedicated vCenter Server instance only to its organization. The tenant does not share the dedicated vCenter Server instance resources with other tenants. Publishing a dedicated vCenter Server instance to multiple tenants violates the tenancy boundaries. However, sometimes a tenant must have access to multiple dedicated vCenter Server instances. In these cases, you can publish a dedicated vCenter Server instance to multiple tenants.

Prerequisites

- Verify that you have at least one vCenter Server instance with enabled tenant access in your VMware Cloud Director environment. See Chapter 9 Managing Dedicated vCenter Server Instances in VMware Cloud Director.

Procedure

1. From the top navigation bar, under **Resources**, click **Infrastructure Resources**.
2. In the left panel, select **vCenter Server Instances**.

3. Select a vCenter Server with enabled tenant access.

   The vCenter Server instances with enabled tenant access have a Dedicated value in the **Usage** column.

4. Click **Manage Tenants**.
5. Select the tenant or tenants to which you want to publish the vCenter Server instance.

   Deselecting a tenant from the list, unpublishes the vCenter Server.

6. Click **Save**.

What to do next

To enable users to access the dedicated vCenter Server instances and the proxies from the VMware Cloud Director Tenant Portal, you must publish the **CPOM extension** plug-in to their organizations. See Publish or Unpublish a Plug-in from a VMware Cloud Director Organization.

Configure Proxy Routing in VMware Cloud Director

Starting with VMware Cloud Director 10.5, you can use the VMware Cloud Director API to manage proxy routing for specific destinations in your environment.

By using the VMware Cloud Director, you can configure rules that specify which proxy to use for access to specific destination hosts, for example, internal identity providers, catalogs, and so on.

Note When a **system administrator** configures system organization proxy routing rules, these rules apply for all tenants in the VMware Cloud Director environment, unless an **organization administrator** configures proxy rules that override them.

When you create a proxy rule for your organization, you configure a backend proxy that is positioned between VMware Cloud Director and the destination host in your environment and functions as an access endpoint for this host.

For details on creating proxy configuration objects, see ProxyConfiguration in VMware Cloud Director OpenAPI Reference.

Procedure

1. Run a GET request to retrieve the VMware Cloud Director provided proxies that are available in your environment.

   ```
   GET  https://{api_host}/cloudapi/1.0.0/proxyConfigurations
   ```

2. Make a note of the URN ID of the proxy configuration that you want to use.
3. To create a proxy rule, run a POST request.

   ```
   POST https://{api_host}/cloudapi/1.0.0/proxyRule
   ```

In the body of the request, include the URN for the proxy, as well the FQDN and port for the destination host for which you want to use it, and credentials, if necessary.

```
{
  "name": "proxy_sample_name",
  "destination": "https://example.intranet.com:10101",
  "proxy": {
    "name": "proxy_name",
    "id": "URN_1"
  },
  "priority": 0
}
```

Here, the value of the `priority` parameter indicates the relative preference of the rule in relation to other rules for the same destination, with lower numerical value indicated higher priority.

View and Edit the Proxy Routing Rules for Your VMware Cloud Director Environment

You can use the VMware Cloud Director OpenAPI to view the existing proxy routing rules for your organization.

Procedure

1 Run a GET request.

```
GET  https://{api_host}/cloudapi/1.0.0/proxyRules
```

The response returns a list of the proxy rules that are configured in your organization.

2 To retrieve details about a specific proxy routing rule, make a note of its ID (URN), and run a GET request.

```
GET  https://{api_host}/cloudapi/1.0.0/proxyRule/proxy_rule_URN
```

3 To update an existing proxy rule, run a PUT request.

```
PUT https://{api_host}/cloudapi/1.0.0/proxyRule/proxy_rule_URN
```

In the body of the request, enter the updated proxy configuration rule.

```
{
  "name": "proxy_sample_name",
  "destination": "https://example.intranet.com:10101",
  "proxy": {
    "name": "proxy_name_2",
    "id": "URN_2"
  },
  "priority": 0
}
```

4 To delete a proxy rule that you don't need anymore, run a DELETE request.

```
DELETE https://{api_host}/cloudapi/1.0.0/proxyRule/proxy_rule_URN
```

Managing System Administrators and Roles in VMware Cloud Director

10

By using the VMware Cloud Director Service Provider Admin Portal, you can add system administrators to VMware Cloud 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.

Note Starting with VMware Cloud Director 9.5, service providers can create provider roles and manage provider users and groups by using the VMware Cloud Director Service Provider Admin Portal or by using the vCloud OpenAPI. For information about managing provider roles, users, and groups, see the *VMware Cloud Director Service Provider Admin Guide*. To examine the vCloud OpenAPI documentation, go to `https://`*`vCloud_Director_IP_address_or_host_name`*`/docs`.

Read the following topics next:

- Managing VMware Cloud Director Rights and Roles
- Managing VMware Cloud Director Provider Users and Groups

Managing VMware Cloud Director Rights and Roles

A right is the fundamental unit of access control in VMware Cloud Director. A role associates a role name with a set of rights. Each organization can have different rights and roles.

VMware Cloud Director uses roles and their associated rights to determine whether a user or group is authorized to perform an operation. Many of the procedures documented in the VMware Cloud Director guides include a prerequisite role. These prerequisites assume that the named role is the unmodified predefined role or a role that includes an equivalent set of rights.

System administrators can use rights bundles and global tenant roles to manage the rights and roles that are available to each organization.

After you install VMware Cloud Director, the system contains only the System Rights Bundle, which includes all rights that are available in the system. The System Rights Bundle is not published to any organization. The system also contains built-in global tenant roles that are published to all organizations. For information about the predefined roles, see Predefined VMware Cloud Director Roles and Their Rights.

After you upgrade VMware Cloud Director from version 9.1 or earlier, in addition to the System Rights Bundle, the system contains a Legacy Rights Bundle for each existing organization. Each Legacy Rights Bundle includes the rights that are available in the associated organization at the time of the upgrade and is published only to this organization.

Note To begin using the rights bundles model for an existing organization, you must delete the corresponding Legacy Rights Bundle.

If you upgraded VMware Cloud Director from version 9.1 or earlier, the existing role templates are published to all organizations as global tenant roles, and the existing roles that are unlinked from role templates are available as tenant-specific roles to their organizations.

Rights Terminology

Right

Each right provides view or manage access to a particular object type in VMware Cloud Director. Rights belong to different categories depending on the objects to which they relate, for example, vApp, Catalog, Organization, and so on. The Provider organization contains all rights available in the system. The system administrator defines the rights that are available to each organization. You cannot create or modify the rights included in VMware Cloud Director.

Rights Bundle

System administrators can use rights bundles to manage the rights that are available to each organization. A rights bundle is a set of rights that the system administrator can publish to one or more organizations. The system administrator can create and publish rights bundles that correspond to tiers of service, separately monetizable functionality, or any other arbitrary rights grouping. Only system administrators can view and manage the rights bundles. You can publish multiple bundles to the same organization.

Organization Rights

Organization rights are the full set of rights that are available to an organization. Organization rights can comprise multiple rights bundles, but the organization administrators and users see a flat set of rights that they can use to create and modify tenant-specific roles.

Roles Terminology

Role

A role is a set of rights that is assignable to one or more users and groups. When you create or import a user or group, you must assign it a role.

Provider Roles

Provider roles are the set of roles that are available only to the Provider organization. Provider roles can be assigned only to Provider users. System administrators can create custom provider roles.

Tenant Roles

Tenant roles are the set of roles available to an organization.

System administrators can create and edit global tenant roles and publish them to one or more organizations. Global tenant roles can be assigned to tenant users in the organizations to which they are published. Organization administrators cannot edit global tenant roles.

Note Tenant users can use only those rights from their roles that are published to their organizations.

Tenant-Specific Roles

Organization administrators can create and edit tenant-specific roles, which are local to their organizations. Tenant-specific roles can be assigned only to tenant users in the organization to which they belong. Tenant-specific roles can contain a subset of the organization rights only.

For information about managing tenant-specific roles, see *VMware Cloud Director Tenant Guide*.

Predefined VMware Cloud Director Roles and Their Rights

Each VMware Cloud 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. For a list of rights available only to the **System administrator** role, see System Administrator Rights in VMware Cloud Director. 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 Cloud Director OpenAPI 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 an OAuth Identity Provider defines the user, the user is assigned the roles named in the `roles` array of the user's OAuth token.
- If a SAML Identity Provider defines the user, 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

A **System Administrator** can use the Service Provider Admin Portal to view the list of rights included in a role.

1. In the top navigation bar, click **Administration**.
2. From the left panel under **Provider Access Control**, select **Roles**.
3. Click the name of the role you want to view.

An **Organization Administrator** can use the Service Provider Admin Portal or the Cloud Director OpenAPI to view the rights in a role or create roles local to the organization.

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**. For a list of the rights in predefined tenant roles, see VMware Cloud Director Rights in Predefined Global Tenant Roles.

System Administrator Rights in VMware Cloud Director

The **System Administrator** role exists only in the provider organization. By default, the **System Administrator** role has all VMware Cloud Director rights.

The **System Administrator** role has all VMware Cloud Director rights. This list consists of the rights available only to **System Administrators**. The **System Administrator** role has also the VMware Cloud Director Rights in Predefined Global Tenant Roles.

The rights' names in the table below are the VMware Cloud Director API rights' names. The API and UI rights' names might be different. If you want to see a list of all VMware Cloud Director rights with API rights' names, UI rights' names, UI right categories, and so on, see the VMware Cloud Director 10.5.x Rights file in CSV format.

Table 10-1. Rights Available by Default Only to System Administrators

New in this release	Right Name
	Access All Organization VDCs
	Access Control List: Manage

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Access Control List: View
	Access Metrics Endpoint
	Additional Services: Execute Workflows
	Additional Services: View Running Workflows
	Additional Services: View Workflows
	Adopt Resource Pool: View
	Advisory Definitions: Create and Delete
	Advisory Definitions: Read
	Allowed Origins: Manage
	Allowed Origins: View
	Alternate Admin Entity: View
	AMQP Settings: Manage
	AMQP Settings: View
	API Explorer: View
	API Tokens: Manage
	API Tokens: Manage All
✓	Catalog Content Source: Change Owner
✓	Catalog Content Source: Delete
✓	Catalog Content Source: Edit
✓	Catalog Content Source: Sharing
✓	Catalog Content Source: View
✓	Catalog Content Source: View ACL
	Catalog: Add vApp from My Cloud
	Catalog: Change Owner
	Catalog: Create / Delete a Catalog
	Catalog: Edit Properties
	Catalog: Import Media from vSphere
	Catalog: Publish

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Catalog: Shadow VM View
	Catalog: Sharing
	Catalog: VCSP Publish Subscribe
	Catalog: VCSP Publish Subscribe Caching
	Catalog: View ACL
	Catalog: View Private and Shared Catalogs
	Catalog: View Published Catalogs
✓	Cell Configuration: Edit
	Cell Configuration: View
	Certificate Library: Manage
	Certificate Library: View
✓	Container App: Manage
✓	Container App: Reconcile App
✓	Container App: View
	Content Library System Settings: Manage
	Content Library System Settings: View
	Custom entity: Create custom entity definitions
	Custom entity: Delete custom entity definitions
	Custom entity: Edit custom entity definitions
✓	Custom entity: Manage any custom entity definition
	Custom entity: View all custom entity instances in org
✓	Custom entity: View any custom entity definition
	Custom entity: View custom entity definitions
	Custom entity: View custom entity instance
	Datastore: Delete
	Datastore: Edit
	Datastore: Enable or Disable
	Datastore: Open in vSphere

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Datastore: View
	Direct Org vDC Network: Manage
	Distributed Virtual Switch: Open in vSphere
	Edge Cluster: Manage
	Edge Cluster: View
	Extension Service API Definition: Manage
	Extension Service API Definition: View
	Extension Services: View
	Extensions: View
	External Service: Manage
	External Service: View
	General ACL: Manage
	General ACL: View
	General: Administrator Control
	General: Administrator View
	General: Send Notification
	General: View Error Details
	Global Role: Edit
	Global Role: View
	Group / User: Manage
	Group / User: View
	Host: Enable or Disable
	Host: Manage
	Host: Open in vSphere
	Host: Prepare or Unprepare
	Host: Repair
	Host: Upgrade
	Host: View

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
✓	IP Spaces Default Gateway Services: Manage
	IP Spaces: Allocate
	Kerberos Settings: Manage
	Kerberos Settings: View
	LDAP Settings: Manage
	LDAP Settings: View
	License Report: View
	Load Balancer Controller: Edit
	Load Balancer Controller: View
	Load Balancer Service Engine Group Assignment: Edit
	Load Balancer Service Engine Group Assignment: View
	Load Balancer Service Engine Group: Edit
	Load Balancer Service Engine Group: View
	Localization Resources: Manage
	Metadata File Entry: Create/Modify
	Network Pool: Create or Delete
	Network Pool: Edit
	Network Pool: Open in vSphere
	Network Pool: Repair
	Network Pool: View
	NSX-T: Edit
	NSX-T: View
	Object Extensions: Manage
	Object Extensions: View
	OIDC Server: Enablement
	OIDC Server: Manage
	Organization Network: Create or Delete
	Organization Network: Edit Properties

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Organization Network: Open in vSphere
	Organization Network: View
	Organization Quotas: Manage
	Organization vDC Compute Policy: Admin View
	Organization vDC Compute Policy: Manage
	Organization vDC Compute Policy: View
✓	Organization vDC Disk: Edit IOPS
	Organization vDC Disk: View IOPS
	Organization vDC Distributed Firewall: Configure Rules
	Organization vDC Distributed Firewall: Enable/Disable
	Organization vDC Distributed Firewall: View Rules
	Organization vDC Gateway: Configure BGP Routing
	Organization vDC Gateway: Configure DHCP
	Organization vDC Gateway: Configure DNS
	Organization vDC Gateway: Configure ECMP Routing
	Organization vDC Gateway: Configure Firewall
	Organization vDC Gateway: Configure IPSec VPN
	Organization vDC Gateway: Configure L2 VPN
	Organization vDC Gateway: Configure Load Balancer
	Organization vDC Gateway: Configure NAT
	Organization vDC Gateway: Configure OSPF Routing
	Organization vDC Gateway: Configure Remote Access
	Organization vDC Gateway: Configure Route Advertisement
	Organization vDC Gateway: Configure SLAAC Profile
	Organization vDC Gateway: Configure SSL VPN
	Organization vDC Gateway: Configure Static Routing
	Organization vDC Gateway: Configure Syslog
	Organization vDC Gateway: Configure System Logging

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Organization vDC Gateway: Convert to Advanced Networking
	Organization vDC Gateway: Create
	Organization vDC Gateway: Delete
	Organization vDC Gateway: Distributed Routing
	Organization vDC Gateway: Import
	Organization vDC Gateway: Modify Form Factor
	Organization vDC Gateway: Update
	Organization vDC Gateway: Update Properties
	Organization vDC Gateway: Upgrade
	Organization vDC Gateway: View
	Organization vDC Gateway: View BGP Routing
	Organization vDC Gateway: View DHCP
	Organization vDC Gateway: View DNS
	Organization vDC Gateway: View Firewall
	Organization vDC Gateway: View IPSec VPN
	Organization vDC Gateway: View L2 VPN
	Organization vDC Gateway: View Load Balancer
	Organization vDC Gateway: View NAT
	Organization vDC Gateway: View OSPF Routing
	Organization vDC Gateway: View Remote Access
	Organization vDC Gateway: View Route Advertisement
	Organization vDC Gateway: View SLAAC Profile
	Organization vDC Gateway: View SSL VPN
	Organization vDC Gateway: View Static Routing
	Organization vDC Kubernetes Policy: Edit
	Organization vDC Named Disk: Change Owner
	Organization vDC Named Disk: Create
	Organization vDC Named Disk: Delete

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Organization vDC Named Disk: Edit Properties
	Organization vDC Named Disk: Move
	Organization vDC Named Disk: View Encryption Status
	Organization vDC Named Disk: View Properties
	Organization vDC Network: Edit Properties
	Organization vDC Network: Import
	Organization vDC Network: View
	Organization vDC Resource Pool: Open in vSphere
	Organization vDC Resource Pool: View
	Organization vDC Shared Named Disk: Create
	Organization vDC Storage Policy: Edit
	Organization vDC Storage Policy: Enable or Disable
	Organization vDC Storage Policy: Open in vSphere
	Organization vDC Storage Policy: Remove
	Organization vDC Storage Policy: View Capabilities
	Organization vDC Storage Profile: Set Default
	Organization vDC: Create
	Organization vDC: Delete
	Organization vDC: Edit ACL
	Organization vDC: Enable or Disable
	Organization vDC: Extended Edit
	Organization vDC: Extended View
	Organization vDC: Manage Firewall
✓ (Available in version 10.5.1 and later)	Organization vDC: Migrate Storage
	Organization vDC: Simple Edit
	Organization vDC: User View
	Organization vDC: View ACL

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Organization vDC: View CPU and Memory Reservation
	Organization VDC: view metrics
	Organization vDC: VM-VM Affinity Edit
	Organization: Activate or Deactivate
	Organization: Create or Delete
	Organization: Edit Association Settings
	Organization: Edit Federation Settings
	Organization: Edit LDAP Settings
	Organization: Edit Leases Policy
	Organization: Edit Limits
	Organization: Edit Name
	Organization: Edit OAuth Settings
	Organization: Edit Password Policy
	Organization: Edit Properties
	Organization: Edit Quotas Policy
	Organization: Edit SMTP Settings
	Organization: Import User/Group from IdP while Editing VDC ACL
	Organization: Migrate Tenant Storage
	Organization: Perform Administrator Queries
✓ (Available in version 10.5.1 and later)	Organization: Traversal
	Organization: Use Provider LDAP as Tenant
	Organization: View
✓	Organization: View Association Settings
	Organization: view metrics
	Port Group: Open in vSphere
	Preference: Manage preference definition
	Private IP Spaces: Manage

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Private IP Spaces: View
✓ (Available in version 10.5.1 and later)	**Provider Gateway BGP: Simple Manage**
✓ (Available in version 10.5.1 and later)	**Provider Gateway BGP: Simple View**
✓ (Available in version 10.5.1 and later)	**Provider Gateway Firewall: Manage**
✓ (Available in version 10.5.1 and later)	**Provider Gateway Firewall: View**
✓ (Available in version 10.5.1 and later)	**Provider Gateway NAT: Manage**
✓ (Available in version 10.5.1 and later)	**Provider Gateway NAT: View**
✓	**Provider Gateway Routing: Manage**
✓	**Provider Gateway Routing: View**
	Provider Gateway: Simple View
	Provider Network: Create or Delete
	Provider Network: Edit
	Provider Network: Open in vSphere
	Provider Network: View
	Provider vDC Compute Policy: Manage
	Provider vDC Compute Policy: View
	Provider vDC Resource Pool: Migrate VMs
	Provider vDC Resource Pool: Open in vSphere
	Provider vDC Resource Pool: View
	Provider vDC Storage Policy: Edit
	Provider vDC Storage Policy: Enable or Disable
	Provider vDC Storage Policy: Open in vSphere

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Provider vDC Storage Policy: Remove
	Provider vDC Storage Policy: View
	Provider vDC: Add Resource Pool
	Provider vDC: Create or Delete
	Provider vDC: Delete Resource Pool
	Provider vDC: Edit
	Provider vDC: Enable or Disable
	Provider vDC: Enable or Disable Resource Pool
	Provider vDC: Enable vSphere VXLAN
	Provider vDC: Merge
	Provider vDC: View
✓	Public Endpoints: Manage
	Quota Policy Capabilities: View
	Quota Policy: Manage
	Quota Policy: View
	Reload VM: Manage
✓	Replication Tracking VM: Manage
	Resource Class Action: Manage
	Resource Class Action: View
	Resource Pool: Open
	Resource Pool: Open in vSphere
	Resource Pool: View
	Right: Manage
	Right: View
	Rights Bundle: Edit
	Rights Bundle: View
	Role: Create, Edit, Delete, or Copy
	SDDC: Manage

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	SDDC: Manage Proxy
	SDDC: View
	Security Tag Edit
	Segment Profile Templates: Manage
	Segment Profile Templates: View
	Selector Extensions: Manage
	Selector Extensions: View
	Service Account: Manage
	Service Account: Simple View
	Service Account: View
	Service Apps: Manage
	Service Apps: View
	Service Authorization: Manage
	Service Configuration: Manage
	Service Configuration: View
	Service Library: Create service libraries
	Service Library: Delete services from the service library
	Service Library: Edit service metadata
	Service Library: Edit the contents of a service
	Service Library: View service libraries
	Service Link: Manage
	Service Link: View
	Service Resource Type: Manage
	Service Resource Type: View
	Service Resource: Manage
	Service Resource: View
	Shared Org vDC Network: Manage
	Site: Edit

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	Site: View
	SSL Settings: View
	SSL Settings: Manage
	SSL: Test Connection
	Stranded Item: Manage
	Stranded Item: View
	Supported Storage Entity Type: Manage
	System IP Spaces: Manage
	System IP Spaces: View
	System Operations: Execute System Operations
	System Organization: Manage
	System Organization: View
	System Settings: Manage
	System Settings: View
✓	System: Manage Proxy Rules
✓	System: View Proxy Rules
	Tanzu Kubernetes Guest Cluster: Administrator Full Control
	Tanzu Kubernetes Guest Cluster: Administrator View
	Tanzu Kubernetes Guest Cluster: Edit
	Tanzu Kubernetes Guest Cluster: Full Control
	Tanzu Kubernetes Guest Cluster: View
	Task: Resume, Abort, or Fail
	Task: Update
	Task: View Tasks
	Token: Manage
	Token: Manage All
	Truststore: Manage
	Truststore: View

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	UI Plugins: Define, Upload, Modify, Delete, Associate or Disassociate
	UI Plugins: View
	UI Portal Branding: Manage
	vApp Template / Media: Copy
	vApp Template / Media: Create / Upload
	vApp Template / Media: Edit
	vApp Template / Media: View
	vApp Template: Add to My Cloud
	vApp Template: Change Owner
	vApp Template: Download
	vApp Template: Force storage lease expiration
	vApp Template: Import
	vApp Template: Open in vSphere
	vApp: Allow All Extra Config
	vApp: Allow Ethernet Coalescing Extra Config
	vApp: Allow Latency Extra Config
	vApp: Allow Matching Extra Config
	vApp: Allow NUMA Node Affinity Extra Config
	vApp: Change Owner
	vApp: Copy
	vApp: Create / Reconfigure
	vApp: Delete
	vApp: Download
	vApp: Edit Properties
	vApp: Edit VM Compute Policy
	vApp: Edit VM CPU
	vApp: Edit VM CPU and Memory reservation settings in all VDC types
	vApp: Edit VM Hard Disk

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	vApp: Edit VM Memory
	vApp: Edit VM Network
	vApp: Edit VM Properties
	vApp: Enter/Exit Maintenance Mode
	vApp: Force runtime lease expiration
	vApp: Force storage lease expiration
	vApp: Import Options
	vApp: Maintenance manage
	vApp: Manage VM Password Settings
	vApp: Open in vSphere
	vApp: Power Operations
	vApp: Shadow VM View
	vApp: Sharing
	vApp: Snapshot Operations
	vApp: Upload
	vApp: Use Console
	vApp: View ACL
	vApp: View VM and VM's Disks Encryption Status
	vApp: View VM Metrics
	vApp: VM Boot Options
	vApp: VM Check Compliance
	vApp: VM Migrate, Force Undeploy, Relocate, Consolidate
	VAPP_VM_METADATA_TO_VCENTER
	VCD Extension: Register, Unregister, Refresh, Associate or Disassociate
	VCD Extension: View
	vCenter: Attach or Detach
	vCenter: Enable or Disable
	vCenter: Open in vSphere

Table 10-1. Rights Available by Default Only to System Administrators (continued)

New in this release	Right Name
	vCenter: Refresh
	vCenter: View
	vDC Group: Configure
	vDC Group: Configure Logging
	vDC Group: View
	VDC Template: ACL manage
	VDC Template: Extended View
	VDC Template: Instantiate
	VDC Template: Manage
	VDC Template: View
	vGPU Profile Consumption: View
	vGPU Profile: Delete
	vGPU Profile: Manage
	vGPU Profile: View
	VMC: Register SDDC
	VMWARE:NATIVECLUSTER: Administrator Full Control
	VMWARE:NATIVECLUSTER: Administrator View
	VMWARE:NATIVECLUSTER: Edit
	VMWARE:NATIVECLUSTER: Full Control
	VMWARE:NATIVECLUSTER: View
	vRealize Orchestrator: Publish and Unpublish Workflows to Tenants
	vRealize Orchestrator: Register and Unregister vRealize Orchestrator Servers
	vRealize Orchestrator: View RegisteredvRealize Orchestrator Servers
	vSphere Server: Manage
	vSphere Server: Manage Proxy
	vSphere Server: Manage Proxy Configuration
	vSphere Server: View

VMware Cloud Director Rights in Predefined Global Tenant Roles

Various VMware Cloud Director 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**.

Rights Included in the Global Tenant Roles in VMware Cloud Director

This list consists of the rights available to user roles in the VMware Cloud Director Tenant Portal. For the rights available to **System Administrators**, see System Administrator Rights in VMware Cloud Director.

The rights' names in the table below are the VMware Cloud Director API rights' names. The API and UI rights' names might be different. If you want to see a list of all VMware Cloud Director rights with API rights' names, UI rights' names, UI right categories, and so on, see the VMware Cloud Director 10.5.x Rights file in CSV format.

New in this release	Right Name	Organization Administrato r	Catalog Author	vApp Author	vApp User	Console Access Only
	Access All Organization VDCs	✓				
	API Tokens: Manage	✓				
	API Tokens: Manage All	✓				
✓	Catalog Content Source: Change Owner	✓				
✓	Catalog Content Source: Delete	✓				
✓	Catalog Content Source: Edit	✓				
✓	Catalog Content Source: Sharing	✓				
✓	Catalog Content Source: View	✓				
✓	Catalog Content Source: View ACL	✓				
	Catalog: Add vApp from My Cloud	✓	✓	✓		
	Catalog: Change Owner	✓				
	Catalog: Create / Delete a Catalog	✓	✓			
	Catalog: Edit Properties	✓	✓			
	Catalog: Publish	✓	✓			
	Catalog: Sharing	✓	✓			
	Catalog: VCSP Publish Subscribe	✓	✓			

New in this release	Right Name	Organization Administrato r	Catalog Author	vApp Author	vApp User	Console Access Only
	Catalog: View ACL	✓	✓			
	Catalog: View Private and Shared Catalogs	✓	✓	✓		
	Catalog: View Published Catalogs	✓				
	Certificate Library: Manage	✓				
	Certificate Library: View	✓				
✓	Container App: Manage	✓				
✓	Container App: View	✓				
	Custom entity: View all custom entity instances in org	✓				
	Custom entity: View custom entity instance	✓				
	General: Administrator Control	✓				
	General: Administrator View	✓				
	General: Send Notification	✓				
	Group / User: Manage	✓				
	Group / User: View	✓				
	IP Spaces: Allocate	✓				
	Metadata File Entry: Create/ Modify	✓				
	Organization Network: Edit Properties	✓				
	Organization Network: View	✓				
	Organization vDC Compute Policy: View	✓	✓	✓	✓	
✓	Organization vDC Disk: Edit IOPS	✓	✓	✓	✓	
	Organization vDC Disk: View IOPS	✓	✓	✓	✓	
	Organization vDC Distributed Firewall: Configure Rules	✓				
	Organization vDC Distributed Firewall: View Rules	✓				
	Organization vDC Gateway: Configure DHCP	✓				

New in this release	Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
	Organization vDC Gateway: Configure DNS	✓				
	Organization vDC Gateway: Configure ECMP Routing	✓				
	Organization vDC Gateway: Configure Firewall	✓				
	Organization vDC Gateway: Configure IPSec VPN	✓				
	Organization vDC Gateway: Configure Load Balancer	✓				
	Organization vDC Gateway: Configure NAT	✓				
	Organization vDC Gateway: Configure Static Routing	✓				
	Organization vDC Gateway: Configure Syslog	✓				
	Organization vDC Gateway: Convert to Advanced Networking	✓				
	Organization vDC Gateway: View	✓				
	Organization vDC Gateway: View DHCP	✓				
	Organization vDC Gateway: View DNS	✓				
	Organization vDC Gateway: View Firewall	✓				
	Organization vDC Gateway: View IPSec VPN	✓				
	Organization vDC Gateway: View Load Balancer	✓				
	Organization vDC Gateway: View NAT	✓				
	Organization vDC Gateway: View Static Routing	✓				
	Organization vDC Named Disk: Change Owner	✓	✓			
	Organization vDC Named Disk: Create	✓	✓	✓		
	Organization vDC Named Disk: Delete	✓	✓	✓		

New in this release	Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
	Organization vDC Named Disk: Edit Properties	✓	✓	✓		
	Organization vDC Named Disk: Move	✓				
	Organization vDC Named Disk: View Encryption Status	✓		✓		
	Organization vDC Named Disk: View Properties	✓	✓	✓	✓	
	Organization vDC Network: Edit Properties	✓				
	Organization vDC Network: View Properties	✓		✓		
	Organization vDC Storage Policy: View Capabilities	✓				
	Organization vDC Storage Profile: Set Default	✓				
	Organization vDC: Edit ACL	✓				
	Organization vDC: Manage Firewall	✓				
✓ (Available in version 10.5.1 and later)	Organization vDC: Migrate Storage	✓				
	Organization vDC: Simple Edit	✓				
	Organization vDC: User View	✓	✓			
	Organization vDC: View ACL	✓				
	Organization vDC: View CPU and Memory Reservation	✓				
	Organization VDC: view metrics	✓				
	Organization vDC: VM-VM Affinity Edit	✓	✓	✓		
	Organization: Edit Association Settings	✓				
	Organization: Edit Federation Settings	✓				
	Organization: Edit Leases Policy	✓				
	Organization: Edit OAuth Settings	✓				

New in this release	Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
	Organization: Edit Password Policy	✓				
	Organization: Edit Properties	✓				
	Organization: Edit Quotas Policy	✓				
	Organization: Edit SMTP Settings	✓				
	Organization: Import User/Group from IdP while Editing VDC ACL	✓				
	Organization: View	✓	✓	✓		
✓	Organization: View Association Settings	✓	✓			
	Organization: view metrics	✓				
	Private IP Spaces: Manage	✓				
	Private IP Spaces: View	✓				
	Provider Gateway: Simple View	✓				
	Quota Policy Capabilities: View	✓				
	Role: Create, Edit, Delete, or Copy	✓				
	Security Tag Edit	✓				
	Service Library: View service libraries	✓				
	SSL: Test Connection	✓	✓			
	Truststore: Manage	✓				
	Truststore: View	✓				
	UI Plugins: View	✓	✓	✓	✓	
	vApp Template / Media: Copy	✓	✓	✓		
	vApp Template / Media: Create / Upload	✓	✓			
	vApp Template / Media: Edit	✓	✓	✓		
	vApp Template / Media: View	✓	✓	✓	✓	
	vApp Template: Add to My Cloud	✓	✓	✓	✓	
	vApp Template: Change Owner	✓	✓			
	vApp Template: Download	✓	✓			

New in this release	Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
	vApp: Change Owner	✓				
	vApp: Copy	✓	✓	✓	✓	
	vApp: Create / Reconfigure	✓	✓	✓		
	vApp: Delete	✓	✓	✓	✓	
	vApp: Download	✓	✓	✓		
	vApp: Edit Properties	✓	✓	✓	✓	
	vApp: Edit VM Compute Policy	✓	✓	✓		
	vApp: Edit VM CPU	✓	✓	✓		
	vApp: Edit VM Hard Disk	✓	✓	✓		
	vApp: Edit VM Memory	✓	✓	✓		
	vApp: Edit VM Network	✓	✓	✓	✓	
	vApp: Edit VM Properties	✓	✓	✓	✓	
	vApp: Manage VM Password Settings	✓	✓	✓	✓	✓
	vApp: Power Operations	✓	✓	✓	✓	
	vApp: Sharing	✓	✓	✓	✓	
	vApp: Snapshot Operations	✓	✓	✓	✓	
	vApp: Upload	✓	✓	✓		
	vApp: Use Console	✓	✓	✓	✓	✓
	vApp: View ACL	✓	✓	✓	✓	
	vApp: View VM and VM's Disks Encryption Status	✓		✓		
	vApp: View VM metrics	✓		✓	✓	
	vApp: VM Boot Options	✓	✓	✓		
	vApp: VM Metadata to vCenter	✓	✓	✓		
	VDC Group: Configure	✓				
	VDC Group: Configure Logging	✓				
	VDC Group: View	✓				
	VDC Template: Instantiate	✓				

New in this release	Right Name	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
	VDC Template: View	✓				
	vGPU Profile Consumption: View	✓				

Managing Rights Bundles in VMware Cloud Director

As a system administrator, you can create rights bundles and publish them to one and more VMware Cloud Director organizations in your cloud. You can edit and delete existing rights bundles. You can unpublish rights bundles from organizations in your cloud.

Create a Rights Bundle in VMware Cloud Director

You can group a set of rights as a rights bundle which you can publish to one or more VMware Cloud Director organizations in your system.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Tenant Access Control**, select **Rights Bundles**.
3. Click **Add**.
4. Enter a name and, optionally, a description for the new rights bundle.
5. Select the rights that you want to associate with this bundle.

   The rights are grouped in categories and subcategories for view or manage access to the object to which they relate.

   You can select the rights individually, by view or manage by subcategory, or by view or manage globally.

Category	Description
Access Control	Contains rights for viewing and managing organizations, rights, roles, and users.
Administration	Contains rights for viewing and managing general and multisite setting.
Compute	Contains rights for viewing and managing organization and provider VDCs, vApps, organization VDC templates, and VM monitoring.
Extensions	Contains rights for viewing and managing VMware Cloud Director plug-ins and extensions.
Infrastructure	Contains rights for viewing and managing vSphere resources.

Category	Description
Libraries	Contains rights for viewing and managing catalogs and catalog items.
Networking	Contains rights for viewing and managing network resources.

6 Click **Save**.

What to do next

You can publish the newly created rights bundle to one or more organizations in your system. See Publish or Unpublish a Rights Bundle to VMware Cloud Director.

Clone a Rights Bundle Using VMware Cloud Director

You can use an existing rights bundle as a template for the creation of a new bundle.

Prerequisites

Verify that you have the rights to add new roles to VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Select the rights bundle that you want to clone and click **Clone**.

4 In the **Clone Rights Bundle** window, enter a name and description for the cloned bundle.

5 (Optional) To edit the cloned rights, turn on the **Modify Selected Rights** toggle, and select or deselect the rights you want to change for the cloned role.

6 Click **Save**.

Publish or Unpublish a Rights Bundle to VMware Cloud Director

You can publish a rights bundle to one or more VMware Cloud Director organizations in your system. After you publish a rights bundle to an organization, the rights in this bundle become part of the organization set of rights.

Organization rights can comprise multiple rights bundles, but the organization administrators and users see a flat set of rights that they can use to create and modify roles.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Select the radio button next to the target bundle and click **Publish**.

4 To publish the bundle:

   a Select **Publish to Tenants**.

   b Select the organizations to which you want to publish the role.

      - If you want to publish the bundle to all existing and newly created organizations in your system, select **Publish to All Tenants**.
      - If you want to publish the bundle to particular organizations in your system, select the organizations individually.

5 To unpublish the bundle:

   - To unpublish the bundle from all organizations in your system, deselect **Publish to Tenants**.
   - To unpublish the bundle from particular organizations in your system, deselect **Publish to All Tenants**, and deselect the organizations individually.

6 Click **Save**.

Results

The rights in the published bundle are available in the selected organizations and can be used in the roles in these organizations.

The rights in the unpublished role are removed from the selected organizations and cannot be used in the roles in these organizations.

View and Edit a Rights Bundle Using VMware Cloud Director

You can view the rights that are included in a rights bundle. You can modify the name, the description, and the rights of a bundle.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Click the name of the target bundle.

   You can view the rights that are associated with the bundle by expanding the right categories.

4 Edit the bundle and click **Keep**.

Results

If you modified the rights of the bundle, the new set of rights is applied to all organizations to which this rights bundle is published.

Delete a Rights Bundle From VMware Cloud Director

You can remove a rights bundle that you no longer use in your VMware Cloud Director organizations.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Tenant Access Control**, select **Rights Bundles**.
3. Select the radio button next to the target bundle and click **Delete**.
4. To confirm, click **OK**.

Managing Global VMware Cloud Director Tenant Roles

As a system administrator, you can create global tenant roles and publish them to one or more VMware Cloud Director organizations in your cloud. You can edit and delete existing global tenant roles. You can unpublish global tenant roles from individual organizations in your cloud.

After the initial VMware Cloud Director installation and setup, the system contains a set of predefined global tenant that are published to all organizations. See Predefined VMware Cloud Director Roles and Their Rights.

Create a Global Tenant Role in Your VMware Cloud Director

You can create a global tenant role that you can publish to one or more VMware Cloud Director organizations in your system.

After the initial VMware Cloud Director installation and setup, the system contains predefined global tenant roles that are published to all organizations. For information about the predefined roles, see Predefined VMware Cloud Director Roles and Their Rights.

You can add custom global roles to your system.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Tenant Access Control**, select **Global Roles**.
3. Click **Add**.
4. Enter a name and, optionally, a description for the new role.
5. Select the rights that you want to associate with the role.

   The rights are grouped in categories and subcategories for view or manage access to the object to which they relate.

   You can select the rights individually, by view or manage by subcategory, or by view or manage globally.

Category	Description
Access Control	Contains rights for viewing and managing organizations, rights, roles, and users.
Administration	Contains rights for viewing and managing general and multisite setting.
Compute	Contains rights for viewing and managing organization and provider VDCs, vApps, organization VDC templates, and VM monitoring.
Extensions	Contains rights for viewing and managing VMware Cloud Director plug-ins and extensions.
Infrastructure	Contains rights for viewing and managing vSphere resources.
Libraries	Contains rights for viewing and managing catalogs and catalog items.
Networking	Contains rights for viewing and managing network resources.

6 Click **Keep**.

Results

Upon its creation, the new global tenant right is available only to the VMware Cloud Director Provider organization.

What to do next

You can publish the newly created role to one or more organizations in your system. See Publish or Unpublish a Global Tenant Role to Your VMware Cloud Director.

Clone a Global Tenant Role to Your VMware Cloud Director

You can use an existing global tenant role as a template for the creation of a new role.

Prerequisites

Verify that you have the rights to add new roles to VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Global Roles**.

3 Select the role that you want to clone and click **Clone**.

4 In the **Clone Global Role** window, enter a name and description for the cloned role.

5 (Optional) To edit the cloned rights, turn on the **Modify Selected Rights** toggle, and select or deselect the rights you want to change for the cloned role.

6 Click **Save**.

Publish or Unpublish a Global Tenant Role to Your VMware Cloud Director

You can publish a global tenant role to one or more VMware Cloud Director organizations in your system. After you publish a role to an organization, this role becomes a part of the organization set of tenant roles.

Prerequisites

To unpublish a global tenant role from an organization, verify that no user is assigned with this role in the organization.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Global Roles**.

3 Select the radio button next to the target role and click **Publish**.

4 To publish the role:

   a Select **Publish to Tenants**.

   b Select the organizations to which you want to publish the role.

      - If you want to publish the role to all existing and newly created organizations in your system, select **Publish to All Tenants**.
      - If you want to publish the role to particular organizations in your system, select the organizations individually.

5 To unpublish the role:

   - To unpublish the role from all organizations in your system, deselect **Publish to Tenants**.
   - To unpublish the role from particular organizations in your system, deselect **Publish to All Tenants**, and deselect the organizations individually.

6 Click **Save**.

Results

The published role is available in the selected organizations and can be assigned to users in these organizations. Organization administrators cannot edit global tenant roles that are published to their organizations.

The unpublished role is removed from the selected organizations and cannot be assigned to users in these organizations.

View and Edit a Global Tenant Role Using Your VMware Cloud Director

You can view the rights that are included in a global tenant role. You can modify the name, the description, and the rights of a global tenant role.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Tenant Access Control**, select **Global Roles**.
3. Click the name of the target role.

   You can view the rights that are associated with the role by expanding the right categories.
4. To modify the name, the description, or the rights of the role, click **Edit**.
5. Edit the role and click **Keep**.

Results

If you modified the rights of the role, the new set of rights is applied to the users across all organizations that are assigned with this role.

Delete a Global Tenant Role From Your VMware Cloud Director

You can remove a global tenant role that you no longer use in your VMware Cloud Director organizations.

Prerequisites

The global tenant role that you want to delete must not be assigned to any user across all organizations.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Tenant Access Control**, select **Global Roles**.
3. Select the radio button next to the target role and click **Delete**.
4. To confirm, click **OK**.

Managing VMware Cloud Director Provider Roles

You can create and manage roles in your VMware Cloud Director Provider organization.

For information about managing tenant roles, see the *VMware Cloud Director Tenant Guide*.

Create a Provider Role in Your VMware Cloud Director

You can create a role in your VMware Cloud Director Provider organization.

After the initial VMware Cloud Director installation and setup, the system contains predefined roles that are local to the Provider organization and global to all organizations. For information about the predefined roles, see Predefined VMware Cloud Director Roles and Their Rights.

You can add custom provider roles to your Provider organization.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Provider Access Control**, select **Roles**.
3. Click **New**.
4. Enter a name and a description for the new role.
5. Select the rights that you want to associate with the role.

   The rights are grouped in categories and subcategories for view or manage access to the object to which they relate.

   You can select the rights individually, by view or manage by subcategory, or by view or manage globally.

Category	Description
Access Control	Contains rights for viewing and managing organizations, rights, roles, and users.
Administration	Contains rights for viewing and managing general and multisite setting.
Compute	Contains rights for viewing and managing organization and provider VDCs, vApps, organization VDC templates, and VM monitoring.
Extensions	Contains rights for viewing and managing VMware Cloud Director plug-ins and extensions.
Infrastructure	Contains rights for viewing and managing vSphere resources.
Libraries	Contains rights for viewing and managing catalogs and catalog items.
Networking	Contains rights for viewing and managing network resources.

6. Click **Save**.

Results

The newly created role is available for assigning to users in your Provider organization.

Clone a Provider Role to Your VMware Cloud Director

You can use an existing provider role as a template for the creation of a new role.

Prerequisites

Verify that you have the rights to add new roles to VMware Cloud Director.

Procedure

1. From the top navigation bar, select **Administration**.

2 In the left panel, under **Provider Access Control**, select **Roles**.

3 Select the role that you want to clone and click **Clone**.

4 In the **Clone Role** window, enter a name and description for the cloned role.

5 (Optional) To edit the cloned rights, turn on the **Modify Selected Rights** toggle, and select or deselect the rights you want to change for the cloned role.

6 Click **Save**.

View or Edit a Provider Role in Your VMware Cloud Director

You can view the rights that are included in a role that is local to your VMware Cloud Director Provider organization. You can modify the name, the description, and the rights of a role.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Provider Access Control**, select **Roles**.

3 Click the name of the target role.

   You can view the rights that are associated with the role by expanding the right categories.

4 To modify the name, the description, or the rights of the role, click **Edit**.

5 Edit the role and click **Save**.

Results

If you modified the rights of the role, the new set of rights is applied to the users that are assigned with this role.

Delete a Provider Role From Your VMware Cloud Director

You can remove a role that you no longer use in your VMware Cloud Director Provider organization.

Prerequisites

The role that you want to delete must not be assigned to any user.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Provider Access Control**, select **Roles**.

3 Select the radio button next to the target role and click **Delete**.

4 To confirm, click **OK**.

Managing VMware Cloud Director Provider Users and Groups

You can add and import users and groups to your VMware Cloud Director Provider organization.

For information about managing organization users and groups, see the *VMware Cloud Director Tenant Guide*.

Note VMware Cloud Director users can share or transfer ownership of entities to other users within the same organization. For this reason, within an organization, any user can see the other users' basic information, such as user name, full name, description, ID, role, and organization.

Managing Provider Users in Your VMware Cloud Director

You can manage the users in your Provider organization by using the Service Provider Admin Portal.

For information about managing tenant users in organizations, see the *VMware Cloud Director Tenant Guide*.

Create a Provider User in Your VMware Cloud Director

You can create a user in your VMware Cloud Director Provider organization.

During the VMware Cloud Director installation and setup, you create a **system administrator** account. After the initial setup, you can create additional administrators and users to the Provider organization.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click **New**.

4 Enter a user name and password for the new user.

The password must contain at least six characters.

5 Select whether to enable the user upon creation.

6 From the **Available roles** drop-down menu, select a role for the user.

The list of available roles comprises the global roles and the roles that are local to your system organization.

7 (Optional) Enter contact information for the user.

You can enter the full name, email address, phone number, and instant messaging ID.

8 (Optional) Set the quotas for the user.

   a You can set a limit of the virtual machines owned by the user, or select **Unlimited**.

   b You can set a limit of the running virtual machines owned by the user, or select **Unlimited**.

Import Provider Users to Your VMware Cloud Director

You can import users to your VMware Cloud Director Provider organization from a previously configured LDAP or SAML identity provider.

Prerequisites

Configure a System LDAP Connection in Your VMware Cloud Director or Configure Your VMware Cloud Director System to Use a SAML Identity Provider.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click **Import Users**.

4 From the **Source** drop-down menu, select your identity provider type.

   Can be **LDAP** or **SAML**.

   If you configured only one identity provider, this option is hard-coded.

5 Specify the users.

Option	Description
LDAP	a Enter a full or partial name of a user and click **Search**. b From the search results, select the users that you want to import. c From the **Assign Role** drop-down menu, select a role for the imported users.
SAML	a Enter the user names of the users that you want to import in the name identifier format supported by the SAML identity provider. Use a new line for each user name. b From the **Assign Role** drop-down menu, select a role for the imported users.

6 Click **Save**.

Results

You can see the imported users in the list of users.

Edit a Provider User in Your VMware Cloud Director

You can change the password, role, contact information, and quotas of a user in your VMware Cloud Director Provider organization. You cannot change the user name.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click the radio button next to the name of the target user and click **Edit**.

4 Edit the user details and click **Save**.

Activate or Deactivate a Provider User in Your VMware Cloud Director

After you deactivate a user, the user cannot log in to VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click the radio button next to the name of the target user and click **Disable** or **Enable**.

4 If deactivating a user, click **OK** to confirm.

Delete a Provider User From Your VMware Cloud Director

You can remove a user from your VMware Cloud Director Provider organization by deleting the user account.

To delete a stranded user that lost access to the system because their LDAP group was deleted, use the VMware Cloud Director API.

Prerequisites

Deactivate the user that you want to delete. See Activate or Deactivate a Provider User in Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click the radio button next to the name of the target user and click **Delete**.

4 To confirm, click **OK**.

Unlock a Provider User in Your VMware Cloud Director

If you enabled account lockout in your password policy system settings, users might lock their accounts after a certain number of invalid login attempts. Even if the lockout is set with an account lockout interval, you can unlock a user account without waiting for the lock to expire.

For information about configuring the account lockout policy, see Configure the VMware Cloud Director Password Policy.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Provider Access Control**, select **Users**.
3. Click the radio button next to the name of the target user and click **Unlock**.

Managing VMware Cloud Director Provider Groups

You can import, edit, and delete groups from your VMware Cloud Director Provider organization by using the Service Provider Admin Portal.

For information about managing groups in organizations, see the *VMware Cloud Director Tenant Guide*.

Import a Provider Group to Your VMware Cloud Director

You can import groups to your VMware Cloud Director Provider organization from a previously configured LDAP, SAML, or OIDC identity provider.

Prerequisites

Configure a System LDAP Connection in Your VMware Cloud Director, Configure Your VMware Cloud Director System to Use a SAML Identity Provider, or Configure Your System to Use an OpenID Connect Identity Provider Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Provider Access Control**, select **Groups**.
3. Click **Import Groups**.
4. From the **Source** drop-down menu, select your identity provider type.

   The identity provider types can be **LDAP**, **SAML**, or **OIDC**.

   If you configured only one identity provider, this option is hard-coded.

5 Specify the users.

Option	Description
LDAP	a Enter a full or partial name of a group, and click **Search**. b From the search results, select the groups that you want to import. c From the **Assign Role** drop-down menu, select a role for the users in the imported groups.
SAML	a Enter the names of the groups that you want to import in the name identifier format supported by the SAML identity provider. Use a new line for each group name. b From the **Assign Role** drop-down menu, select a role for the users in the imported groups.
OIDC	a Enter the names of the groups that you want to import in the name identifier format supported by the OIDC identity provider. Use a new line for each group name. b From the **Assign Role** drop-down menu, select a role for the users in the imported groups.

6 Click **Save**.

Edit a Provider Group in Your VMware Cloud Director

You can edit the description and change the role of the members of a group that you previously imported to your VMware Cloud Director Provider organization.

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click the radio button next to the name of the target group and click **Edit**.

4 Edit the group details, and click **Save**.

Delete a Provider Group From Your VMware Cloud Director

You can remove a group from your VMware Cloud Director Provider organization

Procedure

1 From the top navigation bar, select **Administration**.

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

3 Click the radio button next to the name of the target group and click **Delete**.

4 To confirm, click **OK**.

Managing Service Accounts in VMware Cloud Director

You can automate the access of third-party applications to VMware Cloud Director by using service accounts.

Sharing

Starting with VMware Cloud Director 10.4.1, if you want to limit the service account information that users can see, you can grant to certain roles only the **Limited Service Accounts View** right. When a user with the **Limited Service Accounts View** right makes a GET request on the service account, in the response, the `softwareId`, `softwareVersion`, `uri`, and `status` of the service account appear as `null`.

Implementation

To provide automated access to VMware Cloud Director, service accounts use Generate an API Access Token Using Your VMware Cloud Director Service Provider Admin Portal . Service accounts are intended for API-based access only. Once you grant access to a service account, the authenticated client application receives their API Token, which is an OAuth refresh token, and an access token, representing its first VMware Cloud Director session, for immediate use. Applications need the API tokens for authenticating with VMware Cloud Director. Access tokens are VMware Cloud Director session tokens (JWT tokens), that applications use to make API requests using the service account. The service accounts for applications use API tokens and thus, have the same restrictions as user API tokens in VMware Cloud Director.

Service accounts are granted access using the "Request Service Account Authorization". This guarantees that only the application that must use the token has sole access to the token and can use it. No other actor can access the token. You, as an **administrator**, manage the access to the service account. However, even **administrators** do not have access to the actual token that grants access. VMware Cloud Director gives the token only to the service account. To accomplish this, VMware Cloud Director relies on a well-known standard. To ensure that you and the application to which you are granting the token are in sync through the grant and token transmission, you can only initiate the API token grant process by knowing the user code for the application.

Unlike user API tokens, API tokens granted to service accounts rotate on every use, as per RFC 6749 section 6. Unused service account API tokens never expire unless you revoke them.

Service accounts can have only one role. In OAuth-compliant APIs, the role is communicated through the scope field as a URL-encoded Uniform Resource Name (URN) with the name of the role. The URN format is `urn:vcloud:role:[`*`roleName`*`]`. See RFC 8141 that describes URN encoding.

Note The device endpoint is unauthenticated. Consider configuring special throttling rules at your load balancer.

Table 10-2. Service Account Statuses

Status	Description
Created	The account is in the initial state after creation.
Requested	There are one or more outstanding requests for access that a requester initiated using a device authorization request.
Granted	An administrator granted an outstanding request and is awaiting the service account polling and fetching of the API token.
Active	The service account fetched the API token and can access VMware Cloud Director using the token.

Limitations

Because the use of service accounts is aimed at third-party applications, service accounts have some limitations.

When using service accounts, applications cannot perform certain tasks.

- Perform user management tasks
- Create API tokens
- Manage other service accounts

When accessing VMware Cloud Director by using a service account, applications have only view rights for the following resources.

- User
- Group
- Roles
- Global roles
- Rights bundles

Applications accessing VMware Cloud Director by using a service account do not have the following rights.

- Token: Manage
- Token: Manage All

Multisite

Starting with VMware Cloud Director 10.4.1, service accounts can manage and monitor multiple, geographically distributed VMware Cloud Director installations or server groups and their organizations as single entities by using the multisite feature. For more information, see Configuring and Managing Multisite Deployments. If a service account is making a request to a different organization from the one that it is authenticated to, verify that the service account exists on the associated organization and that it has the same name and software ID. You must also include a `X-VMWARE-VCLOUD-AUTH-CONTEXT` header that specifies the name of the organization that must fulfill your request. See the information for configuring and managing multisite deployments in the *VMware Cloud Director API Programming Guide*.

Create a Service Account Using Your VMware Cloud Director Service Provider Admin Portal

You can create an account for automated access to VMware Cloud Director by using the Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Provider Access Control**, select **Service Accounts**.

3 Click **New**.

4 Enter a name for the service account.

5 From the **Assign Role** drop-down menu, select a role for the service account.

The list of available roles comprises the local system organization roles or if in a tenant organization, the global roles published to the organization in addition to any local roles in the tenant.

6 Enter a software ID for the service account or generate and enter one using the **Generate Software ID** button.

Service accounts must have software IDs which are unique identifiers, in UUID format, representing the software that is connecting to VMware Cloud Director. This ID would be the same for all versions and instances of a piece of software.

For larger solutions, to retain control over the identity of your service accounts, do not use the **Generate Software ID** option, and generate your own software ID.

7 (Optional) Enter the software version of the system using the service account.

The software version is an optional vendor-specified informational piece of metadata associated with the service account. To track when a piece of software changes, VMware Cloud Director uses the software version . The software version might be useful for identifying a service account.

8 (Optional) Enter a client URI.

The client Uniform Resource Identifier (URI) is a URL to the webpage of the vendor and provides information about the client.

9 Click **Next**.

10 (Optional) Add quotas on the resources you want the service account to manage.

These quotas limit the service account's ability to consume storage and compute resources.

11 Review the service account information, and click **Finish**.

Results

The service account appears on the **Service Accounts** page with status `Created`.

Example

You can create a service account also by using the VMware Cloud Director API. The API request uses the same API endpoint as creating a user API token, but the presence of the `software_id` field indicates the intent to create a service account.

Sample request:

```
POST /oauth/provider/register

Accept:application/json

Content-Type:application/json

Authorization:Bearer eyJhbGciOiJSUzI...7g7rA

Body: {

    "client_name": "exampleServiceAccount",

    "software_id": "bc2528fd-35c4-44e5-a55d-62e5c4bd9c99",

    "scope": "urn:vcloud:role:System%20Administrator",

    "client_uri": "https://www.companyname.com",

    "software_version": "1.0"

}
```

Sample response:

```
{

"client_name": "exampleServiceAccount",

"client_id": "734e3845-1573-4f07-9b6c-b493c9042187",

"grant_types": [

"urn:ietf:params:oauth:grant-type:device_code"

],

"token_endpoint_auth_method": "none",

"client_uri": "https://www.company_name.com",
"software_id": "bc2528fd-35c4-44e5-a55d-62e5c4bd9c99",

"software_version": "1.0",

"scope": "urn:vcloud:role:System%20Administrator"

}
```

What to do next

Copy the client ID that appears in the service account details. To grant access to the service account, you must use the client ID.

Grant Access to a Service Account Using Your VMware Cloud Director Service Provider Admin Portal

After you create a service account and the application requests authorization to receive an access token, you can grant the token by using the VMware Cloud Director Service Provider Admin Portal.

Note If the timeout period expires during this procedure, the service account status in the Service Provider Admin Portal changes back to `Created`, and you must start the procedure again.

Prerequisites

1 Copy the client ID from the service account details in the Service Provider Admin Portal.

2 Verify that the application requesting the account makes an OAuth 2.0 Device Authorization Grant RFC-compliant request to the `https://`*`site.cloud.example.com`*`/oauth/provider/device_authorization` API endpoint. For more information on device authorization requests, see RFC 8628 section 3.1.

Key	Value
`client_ID`	*`Generated_Client_ID`*

Once the application requests access, the service account status in the Service Provider Admin Portal changes to `Requested`. The application receives the device code, user code, and some additional information.

Sample request:

```
POST /oauth/provider/device_authorization
Accept:application/json
Content-Type: application/x-www-form-urlencoded
Body:
client_id=734e3845-1573-4f07-9b6c-b493c9042187
```

Sample response:

```
{
"device_code": "tkhZ0uoUMy5xgjJqRJblIq3-g44xy2Ms6TEpv3Z_fKw",
"user_code": "3VL8-SQVJ",
"verification_uri": "https://[VCD]/provider/administration/access-control/service-
accounts",
"expires_in": 3600,
"interval": 60
}
```

The device must poll at the frequency specified in the above response (in seconds) `/oauth/provider/token` as per the RFC. The device must use the device code until it receives the tokens from VMware Cloud Director, or the request times out.

Sample request:

```
POST: /oauth/provider/token
Accept:application/json
Content-Type: application/x-www-form-urlencoded
Body:
client_id=
734e3845-1573-4f07-9b6c-b493c9042187&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-
type%3Adevice_code&device_code=tkhZ0uoUMy5xgjJqRJblIq3-g44xy2Ms6TEpv3Z_fKw
```

Sample response before granting:

```
{
    "error": "authorization_pending",
    "error_description": "Device authorization request pending",
    "error_uri": null,
    "minorErrorCode": "authorization_pending",
    "message": "Device authorization request pending",
    "stackTrace": null
}
```

Sample response after granting:

```
{
    "access_token": "eyJhbGciOiJSU…HqJaDud1sVA",
    "token_type": "Bearer",
    "expires_in": 2592000,
    "refresh_token": "SsybukUed8SBP2p1AaFiGJhrntQNWZVX"
}
```

If you do not confirm or deny an access request, the user code times out. The timeout period appears in the response of the device authorization request.

VMware Cloud Director grants a primary API token to the application only if the application and the administrator use the device code and user code corresponding to each other.

3 Get the user code from the application. You must enter the code in step 4.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Provider Access Control**, select **Service Accounts**.
3. Click **Review Access Requests**.
4. Enter the user code for the application that you obtained in prerequisite 3, click **Lookup**, and verify the requested access details.
5. Grant access to the application.

   If you deny access to the application, the service account status in the Service Provider Admin Portal changes back to `Created`.

Results

The service request status changes to `Granted`. VMware Cloud Director grants the application linked to the service account its primary API token in the form of an API token. Included in the response, as required by the RFC, is an OAuth access token representing a user session for immediate use by the service account. If the application does not use the OAuth access token immediately, the session times out as per the configured idle session timeout. The service account might also explicitly log out, which is recommended not only for security reasons, but also provides a good test run for the service account to make an API call to VMware Cloud Director. Once the application fetches the API token, the status changes to `Active`.

What to do next

- To change the assigned service account role, software ID, software version, client URI, or quota restrictions, select a service account and click **Edit a Service Account**. The changes take effect at the next token refresh.
- To revoke service account access so that the granted API token granted becomes invalid, click **Revoke**. VMware Cloud Director terminates all active sessions. Revoking an API token does not delete the service account, however, the status of the account changes to `Created`. If the application has already requested access again, the status of the service account changes to `Requested`. You must once again follow the procedure to grant access to the service account for the account to become `Active`.

Managing VMware Cloud Director System Settings

11

A VMware Cloud Director system administrator can control system-wide settings related to LDAP, email notification, licensing, and general system preferences.

Read the following topics next:

Modify VMware Cloud Director General System Settings

VMware Cloud Director includes general system settings related to activity logs, networking, session timeouts, certificates, organization limits, operation limits, and so on. The default settings are appropriate for many environments, but you can modify the settings to meet your needs.

For a list of the properties that you can modify, see General VMware Cloud Director System Settings.

Note For information about changing the date, time, or time zone of the VMware Cloud Director appliance, see https://kb.vmware.com/kb/59674.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Settings**, click **General**.

3 Click **Edit** for the section you want to modify, edit the properties, and click **Save**.

General VMware Cloud Director System Settings

VMware Cloud Director includes general system settings that you can modify to meet your needs.

Table 11-1. General System Settings

Name	Category	Description
`Activity log history to keep`	Activity Log	Number of days of the log history to keep before deleting it. Enter **0** never to delete logs.
`Activity log history shown`	Activity Log	Number of days of the log history to display. To show all activity, enter **0** .
`Display debug information`	Activity Log	Enable this setting to display the debug information in the VMware Cloud Director task log.
`IP address release timeout`	Networking	Number of seconds to keep released IP addresses on hold before making them available for allocation again. This default setting is 2 hours (7200 seconds) to allow old entries to expire from client ARP tables.
`Allow Overlapping External Networks`	Networking	To add external networks that run on the same network segment, select the check box. Enable this setting only if you are using non-VLAN-based methods to isolate your external networks.
`Allow FIPS mode`	Networking	Allows enablement of FIPS mode on Edge Gateways. Requires NSX 6.3 or later. See FIPS Mode in the *VMware NSX for vSphere* documentation.
`Default syslog server settings for networks`	Networking	Enter IP addresses for up to two Syslog servers for networks to use. This setting does not apply to Syslog servers used by cloud cells.

Table 11-1. General System Settings (continued)

Name	Category	Description
`Provider Locale`	Localization	Select a locale for provider activity, including log entries, email alerts, and so on.
`Idle session timeout`	Timeouts	Amount of time the VMware Cloud Director application remains active without a user interaction.
`Maximum session timeout`	Timeouts	Maximum amount of time the VMware Cloud Director application remains active.
`Host refresh frequency`	Timeouts	How often VMware Cloud Director checks whether its ESXi hosts are accessible or inaccessible.
`Host hung timeout`	Timeouts	Select the amount of time to wait before marking a host as hung.
`Transfer session timeout`	Timeouts	Amount of time to wait before failing a paused or canceled upload task, for example upload media or upload vApp template. This timeout does not affect upload tasks that are in progress.
`Enable upload quarantine with a timeout of __ seconds`	Timeouts	Select the check box and enter a timeout number representing the amount of time to quarantine uploaded files.
`Verify vCenter and vSphere SSO certificates`	Certificates	By default, VMware Cloud Director always verifies the certificates and the host names in the vCenter Server certificates. This setting is deprecated and will be removed in a future update or major release. **Important** Do not deactivate this setting.
`Edit Organization Limits`	Organization VDC Limits	Enter the maximum number of organization virtual data centers per organization, or select **Unlimited**.
`Number of resource intensive operations running per user`	Operation Limits	Enter the maximum number of simultaneous resource-intensive operations per user, or select **Unlimited**.
`Number of resource intensive operations to be queued per user (in addition to running)`	Operation Limits	Enter the maximum number of queued resource-intensive operations per user, or select **Unlimited**.
`Number of resource intensive operations running per organization`	Operation Limits	Enter the maximum number of simultaneous resource-intensive operations per organization, or select **Unlimited**.
`Number of resource intensive operations to be queued per organization`	Operation Limits	Enter the maximum number of queued resource-intensive operations per organization, or select **Unlimited**.
`Provide default vApp names`	Other	Select the check box to configure VMware Cloud Director to provide default names for new vApps.

Table 11-1. General System Settings (continued)

Name	Category	Description
`Make Allocation pool Org VDCs elastic`	Other	Select the check box to enable the elastic allocation pool, making all allocation pool organization virtual data centers elastic. Before deselecting this option, ensure all virtual machines for each organization virtual data center have been migrated to a single cluster.
`VM discovery enabled`	Other	By default, each organization VDC automatically discovers vCenter VMs that were created in any resource pool that backs the VDC. Clear to deactivate this setting for all VDCs in the system.

Activate FIPS Mode on the VMware Cloud Director Cells in the Server Group

You can configure VMware Cloud Director on Linux to use FIPS 140-2 validated cryptographic modules and to run in FIPS-compliant mode.

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. The NIST Cryptographic Module Validation Program (CMVP) validates the cryptographic modules compliant with the FIPS 140-2 standards.

The goal of VMware Cloud Director FIPS support is to ease the compliance and security activities in various regulated environments. To learn more about support for FIPS 140-2 in VMware products, see https://www.vmware.com/security/certifications/fips.html.

In VMware Cloud Director, FIPS-validated cryptography is deactivated by default. By activating FIPS mode, you configure VMware Cloud Director to use FIPS 140-2 validated cryptographic modules and to run in FIPS-compliant mode.

Important When you activate FIPS mode, the integration with VMware Aria Automation Orchestrator does not work.

VMware Cloud Director uses the following FIPS 140-2 validated cryptographic modules:

- VMware's BC-FJA (Bouncy Castle FIPS Java API), version 1.0.2.3: Certificate #3673 (under NIST review for 1.0.2.3. Approved for version 1.0.2.1. Corresponding Bouncy Castle FIPS module approved for version 1.0.2.3 per Certificate #3514)
- VMware's OpenSSL FIPS Object Module, version 2.0.20-vmw: Certificate #3857

For information about activating FIPS mode on the VMware Cloud Director appliance, see Activate or Deactivate FIPS Mode on the VMware Cloud Director Appliance.

Prerequisites

- Install and activate the `rng-tools` set of utilities. See https://wiki.archlinux.org/index.php/Rng-tools.

- If metrics collection is activated, verify that the Cassandra certificates follow the X.509 v3 certificate standard and include all the necessary extensions. You must configure Cassandra with the same cipher suites that VMware Cloud Director uses. For information about the allowed SSL ciphers, see Managing the List of Allowed SSL Ciphers.
- If you want to use SAML encryption, you must regenerate one of the key pairs for the existing organizations and re-exchange the SAML metadata. Organizations created with VMware Cloud Director 10.2.x and earlier, have two identical key pairs and you must regenerate one of the key pairs. Organizations created with VMware Cloud Director 10.3 and later have two distinct key pairs and you do not need to regenerate any of them.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Settings**, select **SSL**.
3. Click **Enable**.
4. Confirm that your environment meets all prerequisites to activating FIPS mode.

   If your environment does not meet all prerequisites before starting the FIPS mode configuration, VMware Cloud Director might become inaccessible.
5. To confirm you want to start the process, click **Enable**.

   When the configuration finishes, VMware Cloud Director displays a message to restart your cloud cells.
6. After VMware Cloud Director displays a message to restart your cloud cells, restart every cell in the VMware Cloud Director server group.

What to do next

- Deactivate FIPS mode by clicking **Disable**, and after VMware Cloud Director indicates that the configuration is ready, restart the cells.
- You can view the FIPS status of the active VMware Cloud Director cells by using the `fips-mode` CMT command. See View the FIPS Status of All Active Cells in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.
- To avoid host header injection vulnerabilities, activate host header verification.

  a. Log in directly or by using an SSH client to the VMware Cloud Director console as **root**.

  b. Activate host header verification using the cell management tool.

  ```
  /opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
  vcloud.http.enableHostHeaderCheck -v true
  ```

Configure the VMware Cloud Director System Email Settings

You can edit the system email settings, including configuring the SMTP server settings and VMware Cloud Director notification settings.

VMware Cloud Director requires an SMTP server to send user notifications and system alert emails to system users.

VMware Cloud Director sends system alert emails when it has important information to report. For example, VMware Cloud Director sends an alert when a datastore is running out of space. You can configure VMware Cloud Director to send email alerts to all system administrators or to a specified list of email addresses.

Procedure

1 From the top navigation bar, select **Administration**.

2 From the left pane, under **Settings**, select **Email**, and click **Edit**.

3 Enter the DNS host name or IP address of the SMTP mail server.

4 Enter the SMTP server port number.

5 (Optional) If the SMTP server requires a user name, toggle on the **Requires authentication** option and enter the user name and password for the SMTP account.

6 Select the **Notification Settings** tab.

7 Enter an email address to appear as the sender for VMware Cloud Director emails.

   VMware Cloud Director uses the sender's email address to send runtime and storage lease expiration alerts.

8 (Optional) Enter text for the subject prefix.

9 Select the recipients of the notifications.

   By default, only organization administrators receive the SMTP notifications.

10 Click **Save**.

11 (Optional) Test the SMTP settings.

   a Click **Test**.

   b If you enabled the **Requires authentication** option, enter the SMTP server password.

   c Enter a destination email address and click **Test**.

Change the VMware Cloud Director License

VMware Cloud Director requires a valid license, specified as a serial number, to run. You can modify the licensing information that you entered during the initial VMware Cloud Director configuration.

The VMware Cloud Director product serial number is not the same as your vCenter Server license key. You can obtain a VMware Cloud Director serial number from the VMware License Portal.

Procedure

1. From the top navigation bar, select **Administration**.
2. From the left pane, select **License** and click **Edit**.
3. Enter a new serial number and click **Save**.

Configure the Catalog and LDAP Synchronization in Your VMware Cloud Director

Starting with version 10.3.3, you can edit the catalog and LDAP synchronization settings for all VMware Cloud Director organizations and catalogs, including the refresh rate of the catalog subscriptions and LDAP user information.

Procedure

1. From the top navigation bar, select **Administration**.
2. From the left pane, under **Settings**, select **Synchronization**.
3. Edit the catalog synchronization settings.

   a. Under Catalog, click **Edit**.

   b. Enable the catalog synchronization.

   c. Set the synchronization start and stop times.

   d. Set the synchronization interval.

      The synchronization interval is the refresh rate of the catalog subscriptions.

   e. Click **Save**.
4. Edit the LDAP synchronization settings.

   This is a global setting for the synchronization of LDAP user information for both the service provider and tenant users.

   a. Under LDAP, click **Edit**.

   b. To enable LDAP synchronization, turn on the **Status** toggle.

   c. Set the synchronization start time.

   d. Set the synchronization interval.

   e. Click **Save**.

What to do next

For information about configuring catalog synchronization throttling, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Create an Advisory Dashboard in Your VMware Cloud Director

You can create notifications that appear on top of the UI pages in the VMware Cloud Director Service Provider Admin Portal and the Tenant Portal. The messages can appear to system administrators, the users within an organization, or the users in all organizations.

You cannot edit advisories once you create them.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Settings**, select **Advisories** and click **New**.

3 In the description box, add the text of the notification.

   You can use basic Markdown to add links to the notifications.

4 Select the priority of the message.

   Different priority messages appear as different colors. The notifications appear in the order of their priority. Mandatory advisories cannot be removed or snoozed.

5 Select the period for which you want the notification to appear in the UI.

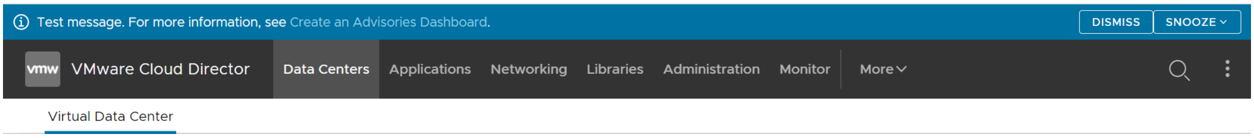
   You can view all advisories in the **Advisories** tab, however they appear to the selected group of users only during the selected period.

6 Select whether you want the notification to appear only to system administrators, to all users within the organization or across organizations.

7 Click **OK**.

Results

The notification appears above the top navigation bar of the selected portal.



Test message. For more information, see Create an Advisories Dashboard.

What to do next

Delete the notification by selecting the radio button next to it and clicking **Delete**. The advisories appear in the **Advisories** tab even after they expire. To remove them from the list, you must delete them.

Configuring and Monitoring Blocking Tasks and Notifications Using Your VMware Cloud Director

You can use blocking tasks and notifications to configure VMware Cloud Director to send AMQP messages triggered by certain events.

Some of these messages are simply notifications that the event has occurred. Other messages publish information to a designated AMQP endpoint indicating that a requested action has been blocked and is pending action by a client application bound to that endpoint. These messages are known as blocking tasks.

A **system administrator** can configure a system-wide set of blocking tasks that are subject to a programmatic action by an AMQP client.

Configure an AMQP Broker Using Your VMware Cloud Director

If you want VMware Cloud Director to send AMQP messages triggered by certain events, you must configure an AMQP broker. You can use the AMQP messages to automate the handling of an underlying user request.

Note Using an AMQP broker will be deprecated in a future VMware Cloud Director release. Consider using an MQTT client instead.

To use an AMQP broker, you must create manually a system exchange in advance. VMware Cloud Director uses the configured system exchange to collect notifications in XML format. VMware Cloud Director publishes notifications in JSON format on an automatically created exchange with a name using the *prefix*.notifications20 format, for example, vcd.notifications20. There are other automatically created exchanges that VMware Cloud Director uses for the API extensibility services. The extension names for these services use the *prefix*.replyExchange format and *prefix*.replyQueue.*cell_UUID* format.

Prerequisites

If you want to use SSL, you can test the connection to the AMQP host and establish a trust relationship with it. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal.

Procedure

1. From the top navigation bar, select **Administration**.
2. Under **Settings**, select **Extensibility**.

   The **AMQP Broker** tab opens.
3. Click the **Edit** button of the **AMQP Broker** section.
4. Enter the DNS host name or IP address of the AMQP host.

   The fully qualified domain name of the RabbitMQ server host, for example, *amqp.example.com*.
5. Enter the AMQP port.

   The default port at which the broker listens to messages is 5672.

6 Enter the exchange.

The exchange is the central point in RabbitMQ, where VMware Cloud Director directs all messages. After installing the broker for VMware Cloud Director, you must access the RabbitMQ management UI at **`http://<HOSTNAME>:15672/`** and create the exchange in the RabbitMQ environment.

The exchange type must be `topic` and the exchange durability must be `durable`. The minimum account permissions can be `publish`, `subscribe`, `create exchange`, and `create queue`.

7 Enter the vHost.

The default is `/`.

8 Enter the prefix.

9 (Optional) To use SSL, turn on the **Use SSL** toggle and select one of the certificate options.

By default, the VMware Cloud Director AMQP service sends unencrypted messages. You can configure the AMQP service to encrypt these messages by using SSL. You can also configure the service to verify the broker certificate by using the default JCEKS trust store of the Java runtime environment on the VMware Cloud Director cell, typically at `$VCLOUD_HOME/jre/lib/security/cacerts`.

Option	Description
SSL Certificate	Upload the SSL certificate.
SSL Key Store (JCEKS)	Upload the SSL keystore and enter the keystore password.

10 Enter a user name and password to connect to the AMQP host.

11 Click **Save**.

12 (Optional) To test the settings, click the **Test** button under the **AMQP Broker** section and provide the password.

The connection test only performs a connection attempt and does not verify the publishing of a message or a check of the exchange configuration.

13 (Optional) To publish audit events to the AMQP broker, click the **Edit** button under the **Non-blocking AMQP Notifications** section and turn on the **Enable notifications** toggle.

Configure Blocking Task Settings On Your VMware Cloud Director

You can configure certain operations as blocking tasks. These operations are suspended until a **system administrator** acts on them or a preconfigured timer expires. You can specify the timeout settings and default actions for blocking tasks. The settings apply to all organizations in the installation.

Procedure

1 From the top navigation bar, select **Administration**.

2 Under **Settings**, select **Extensibility**.

3 Select the **Blocking Tasks** tab.

4 To edit the default extension timeout and default timeout action, click the **Edit** button under the **General** section.

   a Edit the **Default blocking task timeout**.

   b Edit the **Default Timeout Action**.

      The **Default Timeout Action** is the action after a **Default blocking task timeout** expires.

   c Click **Save**.

5 To edit the list of operations, considered as blocking tasks, click the **Edit** button under the **Operations** section.

   a Select or deselect operations from the list of blocking tasks.

   b Click **Save**.

Monitor Blocked Tasks in VMware Cloud Director

You can monitor the current blocked tasks or manually cancel, fail, or resume the tasks before the preconfigured timer expires.

Prerequisites

Configure Blocking Task Settings On Your VMware Cloud Director

Procedure

1 From the top navigation bar, under **Monitor**, select **Blocking Tasks**.

   The tab displays a list of the current blocked tasks.

2 Select the task that you want to edit manually.

3 Decide between canceling, failing, or resuming the task and click the corresponding button.

4 Enter a message and click **Save**.

   The message appears in the task details.

Subscribe to VMware Cloud Director Events, Tasks, and Metrics by Using an MQTT Client

You can use an MQTT client to subscribe to messages about VMware Cloud Director events and tasks.

MQTT is a lightweight, binary, messaging transport protocol. VMware Cloud Director uses MQTT to publish information about events and tasks to which you can subscribe by using an MQTT client. MQTT messages pass through an MQTT broker which can also store messages in case the clients are not online.

Starting with VMware Cloud Director 10.2.2, you can use an MQTT client to subscribe to metrics.

Prerequisites

- Verify that you have an MQTT client that supports WebSocket.
- Verify that you can add headers to a WebSocket-upgraded request.
- If you want to subscribe to metrics, configure the metrics collection and enable metrics publishing. See Configure Metrics Collection and Publishing in VMware Cloud Director.

Procedure

1. Log in to VMware Cloud Director by using the OpenAPI endpoint.
2. To establish a WebSocket connection, set the Sec-WebSocket-Protocol property to `mqtt`, set the client to connect to the `/messaging/mqtt` path, add an authorization header, and follow the standard MQTT connect flow.

   You receive the JWT token from the standard login request to VMware Cloud Director. You can leave the user name and password empty.

   ```
   Sec-WebSocket-Protocol: mqtt
   ```

   ```
   Authorization: Bearer {JWT_token}
   ```

3. Once the connection is established successfully, subscribe to topics through the MQTT client.

   ```
   publish/{user_org_id}/{user_id}
   ```

   ```
   publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
   ```

   Organization administrators can use wildcards to access all organization topics.

   ```
   publish/{user_org_id}/+
   ```

   System administrators can use wildcards to access all topics.

   ```
   publish/#
   ```

4. (Optional) For VMware Cloud Director 10.2.2 or later, subscribe to metrics.

   ```
   metrics/{org_id}/{vApp_id}
   ```

   Only **system administrators** can access the metrics topic.

Configure VMware Cloud Director Public Addresses

To fulfill load balancer or proxy requirements, you can change the default endpoint Web addresses for the VMware Cloud Director Web Portal and VMware Cloud Director API.

Public addresses are Web addresses exposed to clients of VMware Cloud Director. Defaults for these addresses are specified during installation. If necessary, you can update the addresses.

If VMware Cloud Director consists of a single cell, the installer creates public endpoints that usually provide sufficient access for API and Web clients. Installations and deployments that include multiple cells typically place a load balancer between the cells and the clients. Clients access the system at the load balancer's address. The load balancer distributes client requests across the available cells. Other network configurations that include a proxy or place the cells in a DMZ also require customized endpoints. Endpoint URL details are specific to your network configuration.

The endpoints for the VMware Cloud Director Tenant Portal and VMware Cloud Director Web Console require SSL certificates, preferably signed. You must specify a path to these certificates when you install or deploy VMware Cloud Director. If you customize any of these endpoints after installation or deployment, you might need to install new certificates that match endpoint details such as `hostname` and `subject alternative name`.

Starting with VMware Cloud Director 10.4, the console proxy uses the same IP address and port as the REST API. The console proxy and REST API use a single certificate. Because of the unified access point, customizing the VMware Cloud Director public console proxy address is no longer necessary.

Note VMware Cloud Director 10.4.1 and later do not support the legacy implementation of the console proxy feature.

Note If your are using VMware Cloud Director with a load balancer that is configured in SSL-termination mode and you enabled the **LegacyConsoleProxy** feature from the **Feature Flags** settings menu, you must upload the corresponding SSL certificate to secure the console proxy endpoint.

Prerequisites

Verify that you are logged in as a **system administrator**. Only a **system administrator** can customize the public endpoints.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Settings**, click **Public Addresses**.

3 To customize the public endpoints, click **Edit**.

4 To customize the VMware Cloud Director URLs, edit the **Web Portal** endpoints.

   a Enter a custom VMware Cloud Director public URL for HTTP (non-secure) connections.

   b Enter a custom VMware Cloud Director public URL for HTTPS (secure) connections and click **Replace Certificate File** to upload the certificates that establish the trust chain for that endpoint.

   The certificate chain must match the certificate that the service endpoint uses, which is the Web Portal certificate uploaded to each VMware Cloud Director cell. The certificate chain must include an endpoint certificate, intermediate certificates, and a root certificate in the `PEM` format without a private key.

5 Click **Next**.

6 (Optional) To customize the VMware Cloud Director REST API and OpenAPI URLs, turn off the **Use Web Portal Settings** toggle.

   a Enter a custom HTTP base URL.

   For example, if you set the HTTP base URL to **`http://vcloud.example.com`**, you can access the VMware Cloud Director API at `http://vcloud.example.com/api`, and you can access the VMware Cloud Director OpenAPI at `http://vcloud.example.com/cloudapi`.

   b Enter a custom HTTPS REST API base URL and click **Replace Certificate File** to upload the certificates that establish the trust chain for that endpoint.

   For example, if you set the HTTPS REST API base URL to **`https://vcloud.example.com`**, you can access the VMware Cloud Director API at `https://vcloud.example.com/api`, and you can access the VMware Cloud Director OpenAPI at `https://vcloud.example.com/cloudapi`.

   The certificate chain must match the certificate that the service endpoint uses, which is either the HTTP certificate uploaded to each VMware Cloud Director cell or the load balancer VIP certificate if an SSL termination is used. The certificate chain must include an endpoint certificate, intermediate certificates, and a root certificate in the `PEM` format without a private key.

7 If **LegacyConsoleProxy** is enabled, enter a custom VMware Cloud Director public console proxy address.

   - Customize the VMware Cloud Director appliance public console proxy address.

     This address is the fully qualified domain name (FQDN) of the VMware Cloud Director appliance `eth0` NIC, specified either by FQDN or IP address, with custom port `8443` for the console proxy service.

   - Customize the VMware Cloud Director on Linux public console proxy address.

     This address is the fully qualified domain name (FQDN) of the VMware Cloud Director server or load-balancer with the port number. The default port is `443`.

For example, for a VMware Cloud Director appliance instance with FQDN `vcloud.example.com`, enter **`vcloud.example.com:8443`**.

VMware Cloud Director uses the console proxy address when opening a remote console window on a VM.

8 If **LegacyConsoleProxy** is enabled, to secure the communication with the console proxy endpoint, upload a certificate in PEM format.

   a Click **Select certificate file**.

   b Browse to the certificate file on your computer and select it.

9 Click **Save**.

Managing Identity Providers in VMware Cloud Director

You can integrate your VMware Cloud Director with one or more external identity providers (IdPs), and import users and groups to your organizations. You can configure an LDAP server connection at the system or the organization level, a SAML integration at the organization level, and an OpenID Connect (OIDC) integration at the organization level.

An identity provider is a service that manages the user and group identities. VMware Cloud Director organizations that use the same identity provider are federated.

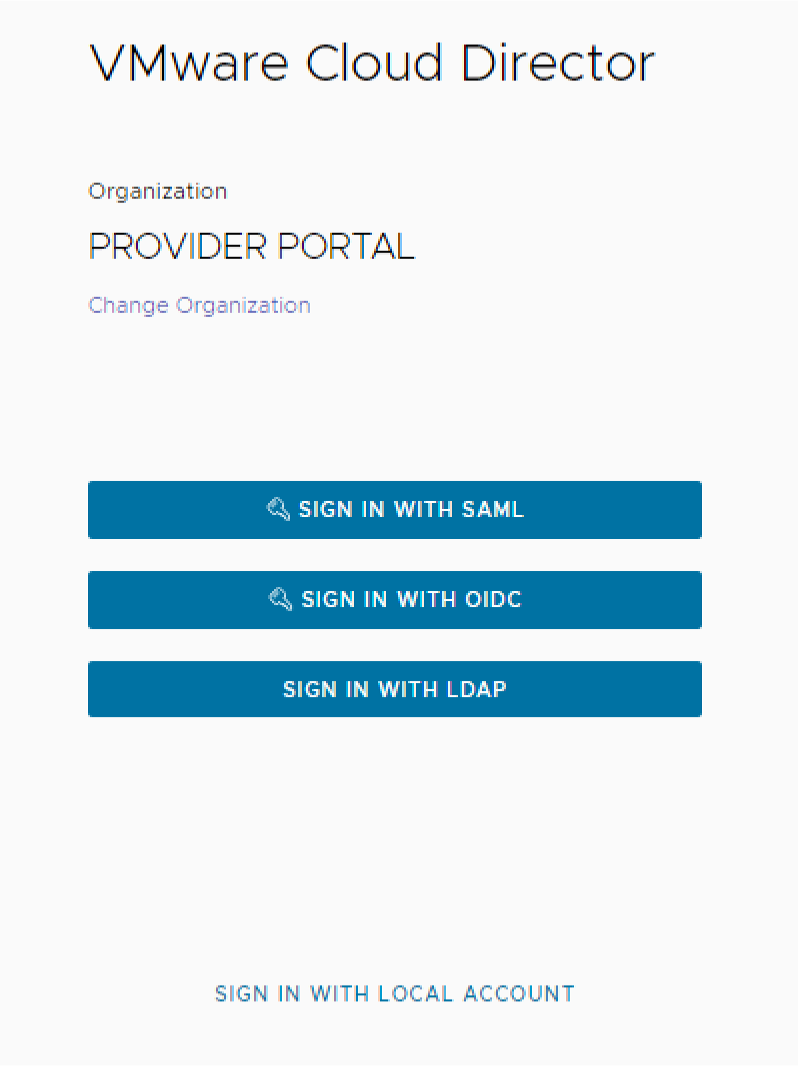
Note For successful VMware Cloud Director integration with external identity providers, to determine the correct values and settings and to ensure proper and accurate configuration, see also the product documentation of those identity providers.

An organization can define an identity provider that it shares with other applications or enterprises. Users authenticate to the identity provider to obtain a token that they can then use to log in to the organization. Such a strategy can enable an enterprise to provide access to multiple, unrelated services, including VMware Cloud Director, with a single set of credentials, an arrangement often referred to as single sign-on.

VMware Cloud Director includes a multisite capability that extends the advantages of a federation by enabling administrators to associate organizations with each other so that a user authenticated to one organization is also authenticated to all organizations that it is associated with. For organizations, sharing of an IdP is a prerequisite to association. See Configuring and Managing Multisite Deployments in Your VMware Cloud Director for more information about associating sites and organizations.

Note Starting with version 10.4.1, VMware Cloud Director starts the deprecation process for local users. VMware Cloud Director continues to fully support the use of local users while they are under deprecation. See VMware Cloud Director 10.4.1 Release Notes.

Starting with version 10.5.1, you can integrate your VMware Cloud Director organizations with more than one identity provider. You must not have identical user names across IdPs. You can have only one integration per IdP technology. For example, you can have one LDAP, one SAML, and one OpenID Connect (OIDC) integration simultaneously. The login page displays all configured sign-in options and to make the login more user friendly, you can customize the button labels from the IdP edit pages.

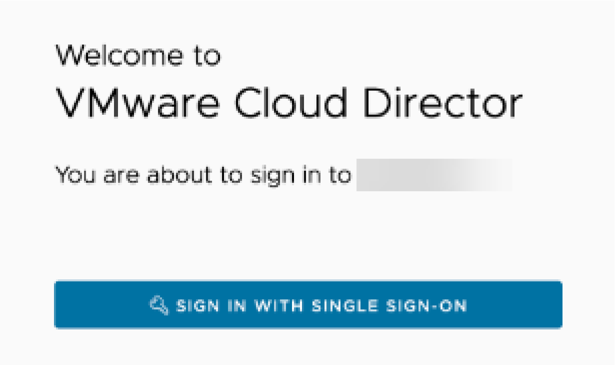


VMware Cloud Director

Organization

PROVIDER PORTAL

Note Only in version 10.5.0, if an organization in VMware Cloud Director has SAML or OIDC configured, the UI displays only the **Sign in with Single Sign-On** option. To log in as a local user in version 10.5.0, navigate to `https://vcloud.example.com/tenant/`*`tenant_name`*`/login` or `https://vcloud.example.com/provider/login`.



Welcome to

VMware Cloud Director

You are about to sign in to [redacted]

Managing LDAP Connections in Your VMware Cloud Director

As a **system administrator**, you can configure your VMware Cloud Director system organization and any other organization in the system to use an LDAP server as a source of users and groups. The organizations can use either the system LDAP connection or a private LDAP connection.

Starting with version 10.1, VMware Cloud Director is moving to a centralized, tenant-aware storage area for certificate management. This way, VMware Cloud Director centralizes all certificates in one place so that **system administrators** and **organization administrators** can view, audit, and manage all certificates in use by various components in the system. You can use the VMware Cloud Director API to add, update, or remove certificates from the new tenant-aware storage area. See *VMware Cloud Director API Schema Reference*.

When adding or editing a new LDAP server endpoint, you can use the VMware Cloud Director UI to test a remote connection to an endpoint and to establish a trust relationship. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal. VMware Cloud Director adds any certificate you decide to trust to a centralized certificate storage area.

Note For successful VMware Cloud Director integration with external identity providers, to determine the correct values and settings and to ensure proper and accurate configuration, see also the product documentation of those identity providers.

Configure a System LDAP Connection in Your VMware Cloud Director

To provide VMware Cloud Director and its organizations with shared access to users and groups, you can configure an LDAP connection at a system level.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Identity Providers**, click **LDAP**.

The current LDAP settings are displayed.

What to do next

Edit, Test, and Synchronize an LDAP Connection Using Your VMware Cloud Director Service Provider Admin Portal .

Configure an Organization LDAP Connection in Your VMware Cloud Director

You can configure a VMware Cloud Director organization to use the system LDAP connection as a shared source of users and groups. You can configure an organization to use a separate LDAP connection as a private source of users and groups.

Procedure

1 From the top navigation bar, select **Resources** and click **Cloud Resources**.

2 In the left panel, select **Organizations**.

3 Click the name of the target organization.

You are redirected to the VMware Cloud Director Tenant Portal of the organization.

4 From the top navigation bar, select **Administration**.

5 In the left panel, under **Identity Providers**, click **LDAP**.

The current LDAP settings are displayed.

6 On the **LDAP Options** tab, click **Edit**.

7 Configure the LDAP source of users and groups for this organization and click **Save**.

Option	Description
Do not use LDAP	The organization does not use an LDAP server as a source of organization users and groups.
VCD system LDAP service	The organization uses the VMware Cloud Director system LDAP connection that you previously configured. See Configure a System LDAP Connection in Your VMware Cloud Director.
Custom LDAP service	The organization uses a private LDAP server as a source of organization users and groups. Click the **Custom LDAP** tab and Edit, Test, and Synchronize an LDAP Connection Using Your VMware Cloud Director Service Provider Admin Portal .

Edit, Test, and Synchronize an LDAP Connection Using Your VMware Cloud Director Service Provider Admin Portal

To configure an LDAP connection, you set the details of your LDAP server. You can test the connection to make sure that you entered the correct settings and the user and group attributes are mapped correctly. When you have a successful LDAP connection, you can synchronize the user and group information with the LDAP server at any time.

Prerequisites

- If you plan to connect to an LDAP server over SSL (LDAPS), verify that the certificate of your LDAP server is compliant with the Endpoint Identification introduced in Java 8 Update 181. The common name (CN) or the subject alternative name (SAN) of the certificate must match the FQDN of the LDAP server. For more information, see the *Java 8 Release Changes* at https://www.java.com.
- If you want to use SSL, you can test the connection to the LDAP server and establish a trust relationship with it. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Identity Providers**, click **LDAP**.

The current LDAP settings are displayed.

3 On the **Custom LDAP** tab, click **Edit**.

4 In the **Connection** tab, enter the required information for the LDAP connection.

Required Information	Description
Server	The host name or IP address of the LDAP server.
Port	The port number on which the LDAP server is listening. For LDAP, the default port number is 389. For LDAPS, the default port number is 636.
Base distinguished name	The base distinguished name (DN) is the location in the LDAP directory where VMware Cloud Director to connect. To connect at root level, enter only the domain components, for example, **`DC=example,DC=com`**. To connect to a node in the domain tree structure, enter the distinguished name for that node, for example, **`OU=ServiceDirector,DC=example,DC=com`**. Connecting to a node limits the scope of the directory available to VMware Cloud Director.
Connector type	The type of your LDAP server. Can be **Active Directory** or **OpenLDAP**.
Use SSL	If your server is LDAPS, select this check box.
Authentication method	Simple authentication consists of sending the user's DN and password to the LDAP server. If you are using LDAP, the LDAP password is sent over the network in plain text. If you want to use Kerberos, you must configure the LDAP connection by using the vCloud API.
User name	Enter the full LDAP distinguished name (DN) of a service account with domain admin rights. VMware Cloud Director uses this account to query the LDAP directory and retrieve user information. If the anonymous read support is enabled on your LDAP server, you can leave these text boxes blank.
Password	The password for the service account that connects to the LDAP server. If the anonymous read support is enabled on your LDAP server, you can leave these text boxes blank.

5 Click the **User Attributes** tab, examine the default values for the user attributes, and, if your LDAP directory uses different schema, modify the values.

6 Click the **Group Attributes** tab, examine the default values for the group attributes, and, if your LDAP directory uses different schema, modify the values.

7 For VMware Cloud Director 10.5.1 and later, if you want to customize the **Sign in with LDAP** button label that appears on the VMware Cloud Director login page, enter a new custom button text.

   You can enter up to 24 symbols. You can use special characters and accented letters. If you want to revert to the default text, delete the custom label. The default button label is localized, and depending on your browser language settings, the text might appear in a different language. Custom labels always appear as you enter them.

8 Click **Save**.

9 If you selected the **Use SSL** check box, and if the certificate of the LDAPS server is not yet trusted, on the **Trust Certificate** window, confirm if you trust the certificate presented by the server endpoint.

10 To test the LDAP connection settings and the LDAP attribute mappings:

   a Click **Test**

   b Enter the password of the LDAP server user that you configured and click **Test**.

      If connected successfully, a green check mark is displayed.

      The retrieved user and group attribute values are displayed in a table. The values that are successfully mapped to LDAP attributes are marked with green check marks. The values that are not mapped LDAP attributes are blank and marked with red exclamation marks.

   c To exit, click **Cancel**.

11 To synchronize VMware Cloud Director with the configured LDAP server, click **Sync**.

   VMware Cloud Director synchronizes the user and group information with the LDAP server regularly depending on the synchronization interval that you set in the general system settings.

   Wait a few minutes for the synchronization to finish.

Results

You can import users and groups from the newly configured LDAP server.

Configure Your VMware Cloud Director System to Use a SAML Identity Provider

If you want to import users and groups from a SAML identity provider to your VMware Cloud Director system organization, you must configure your system organization with this SAML identity provider. Imported users can log in to the system organization with the credentials established in the SAML identity provider.

To configure VMware Cloud Director with a SAML identity provider, you establish a mutual trust by exchanging SAML service provider and identity provider metadata.

Note For successful VMware Cloud Director integration with external identity providers, to determine the correct values and settings and to ensure proper and accurate configuration, see also the product documentation of those identity providers.

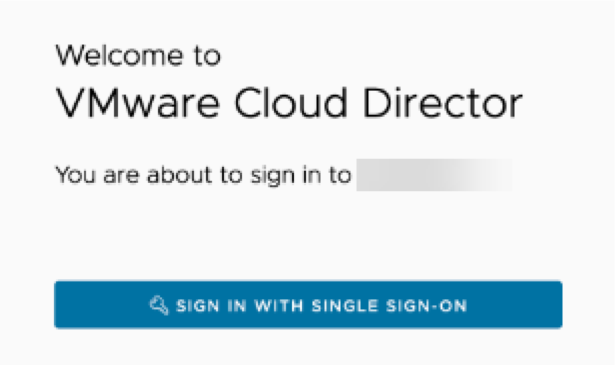
When an imported user attempts to log in, the system extracts the following attributes from the SAML token, if available, and use them for interpreting the corresponding pieces of information about the user.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (this attribute is configurable)

Group information is used if the user is not directly imported but is expected to log in by virtue of membership in imported groups. A user can belong to multiple groups, so 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 using API 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 has no any rights to perform any activities.

Note Only in version 10.5.0, if an organization in VMware Cloud Director has SAML or OIDC configured, the UI displays only the **Sign in with Single Sign-On** option. To log in as a local user in version 10.5.0, navigate to `https://vcloud.example.com/tenant/`*`tenant_name`*`/login` or `https://vcloud.example.com/provider/login`.



Welcome to

VMware Cloud Director

You are about to sign in to [redacted]

Prerequisites

- Verify that you have access to a SAML 2.0 compliant identity provider.

- Obtain an XML file with the following metadata from your SAML identity provider.
  - 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, consult the documentation for your SAML provider.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under Identity Providers, click **SAML** and click **Edit**.

   The current SAML settings are displayed.

3 From the **Service Provider** tab, download the VMware Cloud Director SAML service provider metadata.

   a Enter an Entity ID for the system organization.

      The Entity ID uniquely identifies your system organization to your Identity Provider.

   b Examine the certificate expiration date and, if expiring soon, regenerate the certificate by clicking **Regenerate**.

      The certificate is included in the SAML metadata, and is used for both encryption and signing. Either or both of these might be required depending on how trust is established between your organization and your SAML IDP.

   c Click **Retrieve Metadata**.

      Your browser downloads the SAML service provider metadata, an XML file which you must provide to your identity provider.

4 On the **Identity Provider** tab, upload the SAML metadata that you previously received from your identity provider.

   a Select **Use SAML Identity Provider**.

   b Either click the **Browse** icon and upload the file, or copy and paste its content in the **Metadata XML** text box.

5 For VMware Cloud Director 10.5.1 and later, if you want to customize the **Sign in with SAML** button label that appears on the VMware Cloud Director login page, enter a new custom button text.

   You can enter up to 24 symbols. You can use special characters and accented letters. If you want to revert to the default text, delete the custom label. The default button label is localized, and depending on your browser language settings, the text might appear in a different language. Custom labels always appear as you enter them.

6 Click **Save**.

Configure Your System to Use an OpenID Connect Identity Provider Using Your VMware Cloud Director Service Provider Admin Portal

If you want to import users and groups from an OpenID Connect (OIDC) identity provider to your VMware Cloud Director system organization, you must configure your system organization with this OIDC identity provider. Imported users can log in to the system organization with the credentials established in the OIDC identity provider.

OAuth is an open federation standard that delegates user access. OpenID Connect is an authentication layer on top of the OAuth 2.0 protocol. By using OpenID Connect, clients can receive information about authenticated sessions and end-users. The OAuth authentication endpoint must be reachable from the VMware Cloud Director cells which makes it more suitable when you use public identity providers or provider managed ones.

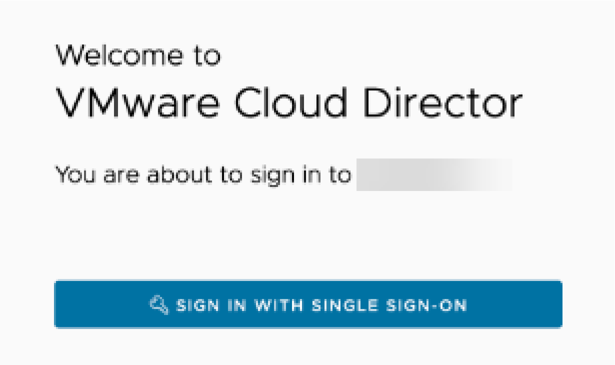
You can allow tenants to generate and issue API access tokens that applications can use on their behalf.

You can configure VMware Cloud Director to automatically refresh your OIDC key configurations from the JWKS endpoint you provide. You can configure the frequency of the key refresh process and the rotation strategy that determines whether VMware Cloud Director adds new keys, replaces the old keys with new, or the old keys expire after a certain period.

Note For successful VMware Cloud Director integration with external identity providers, to determine the correct values and settings and to ensure proper and accurate configuration, see also the product documentation of those identity providers.

VMware Cloud Director generates audit events for both successful and failed key refreshes under the event topic `com/vmware/vcloud/event/oidcSettings/keys/modify`. The audit events for failed key refreshes include additional information about the failure.

Note Only in version 10.5.0, if an organization in VMware Cloud Director has SAML or OIDC configured, the UI displays only the **Sign in with Single Sign-On** option. To log in as a local user in version 10.5.0, navigate to `https://vcloud.example.com/tenant/`*`tenant_name`*`/login` or `https://vcloud.example.com/provider/login`.



Welcome to

VMware Cloud Director

You are about to sign in to

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Identity Providers**, click **OIDC**.

3 If you are configuring OIDC for the first time, copy the client configuration redirect URI and use it to create a client application registration with an identity provider that complies with the OpenID Connect standard, for example, VMware Workspace ONE Access.

   You need this registration to obtain a client ID and a client secret that you must use during the OIDC identity provider configuration.

4 Click **Configure**.

5 Verify that OpenID Connect is active, and enter the client ID and client secret information from the OIDC server registration.

6 (Optional) To use the information from a well-known endpoint to automatically fill in the configuration information, turn on the **Configuration Discovery** toggle and enter a URL at the site of the provider that VMware Cloud Director can use to sent authentication requests to.

7 Click **Next**.

8 If you did not use **Configuration Discovery** in Step 6, enter the information in the **Endpoints** section.

   a Enter the endpoint and issuer ID information.

   b If you are using VMware Workspace ONE Access as an identity provider, select **SCIM** as access type. Starting with VMware Cloud Director 10.4.1, the **SCIM** option is deprecated.

      For other identity providers, you can leave the default **User Info** selection.

   c If you want to combine claims from the `UserInfo` endpoint and the ID Token, turn on the **Prefer ID Token** toggle.

      The identity providers do not provide all the required claims set in the `UserInfo` endpoint. By turning on the **Prefer ID Token** toggle, VMware Cloud Director can fetch and consume claims from both sources.

   d Enter the maximum acceptable clock skew.

      The maximum clock skew is the maximum allowable time difference between the client and server. This time compensates for any small time differences in the timestamps when verifying tokens. The default value is 60 seconds.

   e Click **Next**.

9 If you did not use **Configuration Discovery** in Step 6, enter the scope information, and click **Next**.

   VMware Cloud Director uses the scopes to authorize access to user details. When a client requests an access token, the scopes define the permissions that this token has to access user information.

10 If you are using **User Info** as an access type, map the claims and click **Next**.

You can use this section to map the information VMware Cloud Director gets from the user info endpoint to specific claims. The claims are strings for the field names in the VMware Cloud Director response.

11 If you want VMware Cloud Director to automatically refresh the OIDC key configurations, turn on the **Automatic Key Refresh** toggle.

a If you did not use **Configuration Discovery** in Step 6, enter the **Key Refresh Endpoint**.

The **Key Refresh Endpoint** is a JSON Web Key Set (JWKS) endpoint and it is the endpoint from which VMware Cloud Director fetches the keys.

b Select how often the key refresh occurs.

You can set the period in hourly increments from 1 hour up to 30 days.

c Select a **Key Refresh Strategy**.

Option	Description
Add	Add the incoming set of keys to the existing set of keys. All keys in the merged set are valid and usable. For example, your existing set of keys includes keys A, B, and D. Your incoming set of keys includes keys B, C, and D. When the key refresh occurs, the new set includes keys A, B, C, and D.
Replace	Replace the existing set of keys with the incoming set of keys. For example, your existing set of keys includes keys A, B, and D. Your incoming set of keys includes keys B, C, and D. When the key refresh occurs, key C replaces key A. The incoming keys B, C, and D become the new set of valid keys without any overlap with the old set.
Expire After	You can configure an overlap period between the existing and incoming sets of keys. You can configure the overlapping time using the **Expire Key After Period**, which you can set in hourly increments from 1 hour up to 1 day. The key refresh runs start at the beginning of every hour. When the key refresh occurs, VMware Cloud Director tags as expiring the keys in the existing set of keys that are not included in the incoming set. At the next key refresh run,VMware Cloud Director stops using the expiring keys. Only keys included in the incoming set are valid and usable. For example, your existing set of keys includes keys A, B, and D. The incoming set includes keys B, C, and D. If you configure the existing keys to expire in 1 hour, there is 1 hour overlap during which both sets of keys are valid. VMware Cloud Director marks key A as expiring and until the next key refresh run, keys A, B, C, and D are usable. At the next run, key A expires and only B, C, and D continue working.

12 For VMware Cloud Director 10.5.1 and later, if you did not use **Configuration Discovery** in Step 6, upload the private key that the identity provider uses to sign its tokens.

13 If you want to customize the **Sign in with OIDC** button label that appears on the VMware Cloud Director login page, enter a new custom button text.

You can enter up to 24 symbols. You can use special characters and accented letters. If you want to revert to the default text, delete the custom label. The default button label is localized, and depending on your browser language settings, the text might appear in a different language. Custom labels always appear as you enter them.

14 Click **Save**.

What to do next

- Subscribe to the `com/vmware/vcloud/event/oidcSettings/keys/modify` event topic.
- Verify that the **Last Run** and the **Last Successful Run** are identical. The runs start at the beginning of the hour. The **Last Run** is the time stamp of the last key refresh attempt. The **Last Successful Run** is the time stamp of the last successful key refresh. If the time stamps are different, the automatic key refresh is failing and you can diagnose the problem by reviewing the audit events.

Enable PKCE in VMware Cloud Director

Starting with version 10.5, VMware Cloud Director supports Proof Key for Code Exchange (PKCE).

PKCE is an extension to the OAuth 2.0 Authorization Code flow that is used to prevent CSRF and authorization code injection attacks. For more information, see Proof Key for Code Exchange in the OAuth 2.0 documentation.

For more details on using VMware Cloud Director API for OAuth configuration, see VMware Cloud Director API and Configuring and Managing Federation with OAuth.

Prerequisites

Verify that you configured your system to use an OpenID Connect Identity Provider. See Configure Your System to Use an OpenID Connect Identity Provider Using Your VMware Cloud Director Service Provider Admin Portal.

Procedure

1 Run the request to retrieve your organization's settings.

```
GET https://vcloud.example.com/api/admin/org/organization_id/settings/oauth
```

The response contains the OAuth settings for your organization.

2. Under `OrgOAuthSettings`, make the following changes.

   a. Modify the `usePkce` element to `true`.

   b. (Optional) If your identity provider requires that client credentials be sent as an authorization header when making the API request to retrieve the access token, modify the `sendClientCredentialsAsAuthorizationHeader` element to `true`.

      The default behavior is for the client credentials to be sent in the body of the API request.

3. To update your OAuth settings with your modifications, run a PUT request.

   ```
   PUT https://vcloud.example.com/api/admin/org/organization_id/settings/oauth
   ```

   In the body of the request, include the modified elements of your OAuth settings.

Generate an API Access Token Using Your VMware Cloud Director Service Provider Admin Portal

You can generate and issue API access tokens. You are authenticated using your respective security best practices, including leveraging two-factor authorization, by using API access tokens, you can grant access for building automation against VMware Cloud Director.

Access tokens are artifacts that client applications use to make API requests on behalf of a user. Applications need access tokens for authentication. When an access token expires, to obtain access tokens, applications can use API tokens. API tokens do not expire.

When using access tokens, applications cannot perform certain tasks.

- Change the user password
- Perform user management tasks
- Create more tokens
- View or revoke other tokens

When accessing VMware Cloud Director by using an API access token, applications have only view rights for the following resources.

- User
- Group
- Roles
- Global roles
- Rights bundles

Applications accessing VMware Cloud Director by using an API access token do not have the following rights.

- Token: Manage
- Token: Manage All

Similar to generating a user API token, you can create a service account by using the VMware Cloud Director API. The API request for creating a service account uses the same API endpoint as creating a user API token, but the presence of the `software_id` field indicates the intent to create a service account.

Prerequisites

Authenticating with an API token uses the "Refreshing an Access Token" standard as specified in the OAuth 2.0 RFC 6749 Section 6 to allow access to VMware Cloud Director as an OAuth application. The returned access token is the same as a VMware Cloud Director access token and client applications can use it to make subsequent API calls to VMware Cloud Director. To make an OAuth 2.0 RFC-compliant request, familiarize yourself with Request for Comments (RFC) 6749 Section 6 information about refreshing an access token.

Procedure

1 In the top right corner of the navigation bar, click your user name, and select **User preferences**.

2 Under the **API Tokens** section, click **New**.

3 Enter a name for the token, and click **Create**.

The generated API token appears. You must copy the token because it appears only once. After you click **OK**, you cannot retrieve this token again, you can only revoke it.

4 Make an OAuth 2.0 RFC-compliant request to the `https://site.cloud.example.com/oauth/provider/token` API endpoint.

Key	Value
grant_type	`refresh_token`
refresh_token	*`Generated_refresh_token`*

The request returns an access token that applications can use to perform tasks in VMware Cloud Director. The token is valid even after the user logs out. When an access token expires, the application can obtain more access tokens by using the API token.

Example

Request:

```
POST https://host_name/oauth/provider/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

grant_type=refresh_token&refresh_token=Generated_API_Token
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "access_token":"Generated_Access_Token",
   "token_type":"Bearer",
   "expires_in":2592000,
   "refresh_token":null
}
```

Request using the generated access token:

```
GET https://host_name/api/org
Accept: application/*+xml;version=36.1
Authorization: Bearer Generated_Access_Token
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/vnd.vmware.vcloud.orglist+xml;version=36.1
X-VMWARE-VCLOUD-REQUEST-EXECUTION-TIME: 41

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<OrgList
    xmlns="http://www.vmware.com/vcloud/v1.5"
    xmlns:vmext="http://www.vmware.com/vcloud/extension/v1.5"
    xmlns:ovf="http://schemas.dmtf.org/ovf/envelope/1"
    xmlns:vssd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/
CIM_VirtualSystemSettingData"
    xmlns:common="http://schemas.dmtf.org/wbem/wscim/1/common"
    xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/
CIM_ResourceAllocationSettingData"
    xmlns:vmw="http://www.vmware.com/schema/ovf"
    xmlns:ovfenv="http://schemas.dmtf.org/ovf/environment/1"
    xmlns:ns9="http://www.vmware.com/vcloud/versions" href="https://host_name/api/org/"
type="application/vnd.vmware.vcloud.orgList+xml">
    <Org href="https://host_name/api/org/a93c9db9-7471-3192-8d09-a8f7eeda85f9"
type="application/vnd.vmware.vcloud.org+xml" name="System"/>
</OrgList>
```

What to do next

- If you want tenants to be able to generate tokens, you must grant tenant roles the **Manage user's own API token** right.
- By default, tenants see only the tokens they create. To allow organization administrators to see and revoke the tokens of the other tenant users in the organization, you must grant them the **Manage all users' API tokens** right. Administrators with the **Manage all users' API tokens** right can see only the names of other users' the tokens, not the tokens themselves.

- To revoke any of your tokens, navigate to the **User preferences** page, and click the vertical ellipsis next to the token.
- To revoke the tokens of other users, in the top navigation bar, under **Administration**, navigate to the access control settings for users. When selecting a specific user, you can also see their access tokens and revoke them.
- If you need to identify events triggered by using an API access token, in the event log the following line appears in the `additionalProperties` section of an event.

  ```
  "currentContext.refreshTokenId": "<UUID_of_the_token_that_performed_the_action>",
  ```

Remapping VMware Cloud Director Users Between Identity Providers

You can remap VMware Cloud Director users between identity providers.

You can remap individual users from one identity provider (IDP) to another by using the VMware Cloud Director API. You can use the VMware Cloud Director UI for bulk remapping of users between identity providers.

Remap Users Between Identity Providers Using Your VMware Cloud Director Service Provider Admin Portal

Starting with version 10.4.2, you can use the VMware Cloud Director UI for bulk remapping of users between identity providers.

Note With version 10.4.1, VMware Cloud Director started the deprecation process for local users. VMware Cloud Director continues to fully support the use of local users while they are under deprecation. For more details, see VMware Cloud Director 10.4.1 Release Notes.

Prerequisites

- Verify that your role includes the **Group / User: Manage** right.
- Verify that the organization is configured with the identity provider types that you want to remap between.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Provider Access Control**, select **Users**.
3. Click **Bulk Update**.
4. Click **Export Users**.

   The users are exported into a CSV file.

5 In the CSV file with the users, change the value in the `providerType` field to identify the new IDP for each user.

   VMware Cloud Director supports the `SAML`, `LDAP`, `LOCAL`, and `OAUTH` values. To remap a user to an OIDC identity provider, you must change the value in the `providerType` field to `OAUTH`.

   Note You can remap a user to `LOCAL` identity provider type only by using the VMware Cloud Director API. See Remap a User Between Identity Providers by Using the VMware Cloud Director API

6 (Optional) To match the user name in the IDP that each user is remapping to, modify the user name.

   For VMware Cloud Director to continue to associate the user's assets with the user when they login through the new login flow, the ID of the user must remain unchanged. Changes to all other fields are ignored.

7 Save your changes and close the CSV file.

8 In the **Users Bulk Update** wizard, click **Next**.

9 Click **Select CSV File**, browse to the file and upload it.

10 Click **Next**.

11 Click **Update**.

   When you start the update process, users are remapped one by one. Users for which no changes are detected are skipped. If you close the VMware Cloud Director UI tab while before the process is complete, the update stops.

Remap a User Between Identity Providers by Using the VMware Cloud Director API

Starting with VMware Cloud Director 10.4.1, you can remap individual users from one identity provider (IDP) to another by using the VMware Cloud Director API.

Note VMware Cloud Director starts the deprecation process for local users. VMware Cloud Director continues to fully support the use of local users while they are under deprecation. See VMware Cloud Director 10.4.1 Release Notes.

For information about bulk remapping of users between identity providers by using the VMware Cloud Director UI, see Remap Users Between Identity Providers Using Your VMware Cloud Director Service Provider Admin Portal .

Prerequisites

- Verify that your role includes the **Group / User: Manage** right.
- Verify that the organization is configured with the identity provider types that you want to remap between.

Procedure

1 Make a GET request to `/cloudapi/1.0.0/users`.

VMware Cloud Director returns a list of the users within the organization.

2 Locate the user you want to remap, and retrieve the user information.

```
GET /cloudapi/1.0.0/users/{user_id}
```

3 Make a PUT request to `/cloudapi/1.0.0/users/{user_id}`.

To remap a user, you must change the `providerType` field to identify the new IDP. VMware Cloud Director supports the `SAML`, `LDAP`, `OAUTH`, and `LOCAL` values. Additionally, to match the user name in the IDP that the user is remapping to, you can modify the user name. For VMware Cloud Director to continue to associate the user's assets with the user when they login through the new login flow, the ID of the user must remain unchanged.

Important If you are remapping to provider type `LDAP`, VMware Cloud Director validates the user name with the LDAP server before committing the operation. If VMware Cloud Director does not complete this step for any reason, for example, loss of connectivity to the LDAP server, the remapping fails.

If you are remapping a user to be a local user by specifying provider type `LOCAL`, similar to the process of creating a user, you must provide a password.

4 Verify that VMware Cloud Director returns an `OK` response specifying the newly remapped provider type in the response body.

Example:

To find the user that you want to remap, make the following request.

Request:

```
GET /cloudapi/1.0.0/users?pageSize=10 HTTP/1.1
Host: 127.0.0.1:8443
Accept: application/json;version=37.1
```

Sample response:

```
{
  "resultTotal": 2,
  "pageCount": 1,
  "page": 1,
  "pageSize": 10,
  "associations": null,
  "values": [
    ...,
    {
      "username": "testuser",
      "fullName": "",
      "description": null,
      "id": "urn:vcloud:user:2b038199-0063-4c13-9bba-a3b58d775785",
      "roleEntityRefs": [
        {
          "name": "vApp Author",
          "id": "urn:vcloud:role:85f69506-52a5-3e20-869a-ea18d667e19e"
        }
      ],
      "orgEntityRef": {
        "name": "testorg",
        "id": "urn:vcloud:org:806f0d87-c8b9-47f5-bfbe-3dc73a4c0d14"
      },
      "password": "******",
      "email": "",
      "nameInSource": "testuser",
      "enabled": true,
      "isGroupRole": false,
      "providerType": "LOCAL"
    }
  ]
}
```

To remap `testuser` from `LOCAL` to `LDAP`, make a PUT request.

Request:

```
PUT /cloudapi/1.0.0/users/urn:vcloud:user:2b038199-0063-4c13-9bba-a3b58d775785 HTTP/1.1
Host: 127.0.0.1:8443
Accept: application/json;version=37.1
Content-Type: application/json;version=37.1

Body: {
  "username": "testuser",
  "fullName": "",
  "description": null,
  "id": "urn:vcloud:user:2b038199-0063-4c13-9bba-a3b58d775785",
  "roleEntityRefs": [
    {
      "name": "vApp Author",
      "id": "urn:vcloud:role:85f69506-52a5-3e20-869a-ea18d667e19e"
    }
  ],
  "orgEntityRef": {
    "name": "testorg",
    "id": "urn:vcloud:org:806f0d87-c8b9-47f5-bfbe-3dc73a4c0d14"
  },
  "password": "******",
  "email": "",
  "nameInSource": "testuser",
  "enabled": true,
  "isGroupRole": false,
  "providerType": "LDAP"
}
```

Sample response:

```
{
  "username": "testuser",
  "fullName": "",
  "description": null,
  "id": "urn:vcloud:user:2b038199-0063-4c13-9bba-a3b58d775785",
  "roleEntityRefs": [
    {
      "name": "vApp Author",
      "id": "urn:vcloud:role:85f69506-52a5-3e20-869a-ea18d667e19e"
    }
  ],
  "orgEntityRef": {
    "name": "testorg",
    "id": "urn:vcloud:org:806f0d87-c8b9-47f5-bfbe-3dc73a4c0d14"
  },
  "password": null,
  "email": "",
  "nameInSource": "\\63\\36\\62\\35\\30\\66\\35\\63\\2D\\61\\62\\30\\35\\2D\\34\\37\\64\\33\\2D\\62\\61\\64\\34\\2D\\39\\32\\64\\35\\32\\37\\30\\36\\62\\39\\39\\33",
  "enabled": true,
  "isGroupRole": false,
  "providerType": "LDAP"
}
```

Using VMware Cloud Director as an Identity Provider Proxy Server

Starting with version 10.4.2, you can use VMware Cloud Director as a tenant-aware identity provider proxy server.

When VMware Cloud Director is configured as an identity provider proxy server by using the OAuth 2.0 OpenID Connect standard, relying parties can use VMware Cloud Director for tenant-aware authentication of users known to VMware Cloud Director. For detailed information on the OpenID Connect standard, see OpenID Connect Core 1.0.

As an identity provider proxy server, VMware Cloud Director acts as intermediary between the client application (relying party) and the identity provider, and delegates actual authentication to the respective authentication mechanism used by the provider or tenants.

A **system administrator** can configure relying parties that integrate with VMware Cloud Director and then enable individual tenants to allow their users to use VMware Cloud Director as an identity provider proxy.

Authentication Flow

Integration with VMware Cloud Director is implemented through the OAuth 2.0 OIDC authorization code flow standard. For detailed information, see Authentication using the Authorization Code Flow.

When a relying party redirects a user to VMware Cloud Director, if there is no existing client session, the user is prompted to log in to VMware Cloud Director by first identifying the organization or provider portal they wish to log into. The user authenticates through the configured authentication mechanism, which may involve further redirections to external identity providers. If the user's browser detects an existing VMware Cloud Director user session, the authentication flow provides an SSO experience and no user interaction is required for reauthentication. Upon successful completion of the process, VMware Cloud Director returns an access token and an ID token. The authorization code that is issued as part of the flow is valid for 5 minutes. The access token is valid for 5 minutes, and the ID token is valid for an hour.

Note VMware Cloud Director does not return a refresh token.

You cannot use the access token that VMware Cloud Director returns upon successful authentication for accessing the UI portals or for making regular VMware Cloud Director API calls.

ID Token Details

The ID token that VMware Cloud Director returns contains the following OpenID standard claims and VMware Cloud Director specific claims.

Claim	Description
`at_hash`	(OpenID standard claim) Access token hash value.
`sub`	(OpenID standard claim) The `userId` in VMware Cloud Directorin UUID format.
`iss`	(OpenID standard claim) Public address of VMware Cloud Director.
`preferred_username`	(OpenID standard claim) User name of the user in VMware Cloud Director
`nonce`	(OpenID standard claim) String value used to associate a client session with an ID token, and to mitigate replay attacks. Only present if it was initially included in the relying party request.
`aud`	(OpenID standard claim) The audience for this token. The value is the client ID of requesting relying party.
`azp`	(OpenID standard claim) Authorized party for the token. The value is the client ID of the relying party. Its value is same as the `aud` claim.
`name`	(OpenID standard claim) Full name of the user, if known to VMware Cloud Director.
`phone_number`	(OpenID standard claim) Phone number of the user, if known to VMware Cloud Director.
`exp`	(OpenID standard claim) Expiration time. Time after which the ID token is not accepted for processing.
`iat`	(OpenID standard claim) Time at which the ID token was issued.

Claim	Description
`email`	(OpenID standard claim) Email address of the user, if known to VMware Cloud Director.
`roles`	(VMware Cloud Director custom claim) An array of the names of the roles the user has in VMware Cloud Director.
`groups`	(VMware Cloud Director custom claim) An array of the names of the groups in which the user belongs in VMware Cloud Director.
`org_name`	(VMware Cloud Director custom claim) Name of the organization in which the user is logged in.
`org_display_name`	(VMware Cloud Director custom claim) Display name of the organization.
`org_id`	(VMware Cloud Director custom claim) The organization ID in UUID format.

OpenID Request Scopes

The scope of the OpenID request is used to specify the privileges requested for an access token.

Scope Values	Description.
`openid`	Required. OpenID standard scope.
`profile`	OpenID standard scope. Requests access to the end-user default profile claims.
`email`	OpenID standard scope. Requests access to the end-user email address claims.
`groups`	OpenID standard scope. Requests access to the groups that the user is part of in VMware Cloud Director.
`phone`	OpenID standard scope. Requests access to the user phone number claim.
`vcd_idp`	VMware Cloud Director specific scope. Requests access to VMware Cloud Directorcustom claims, such as `roles`, `groups`, `org_name`, `org_display_name`, and `org_id`.

Endpoints

- You can use the access token returned by VMware Cloud Director to retrieve claims about the authenticated user at the *hostname*`/oidc/UserInfo` endpoint. For details, see UserInfo Endpoint.
- You can retrieve the provider configuration values, including the JWKS endpoint and information about other endpoints and scopes necessary for the OIDC proxy configuration at the well-known configuration URL *hostname*`/oidc/.well-known/openid-configuration`. See View the OIDC Proxy General Settings in Your VMware Cloud Director.

Token Exchange Access to VMware Cloud Director Identity Provider Proxy

Programmatic integration with the identity provider proxy functionality of VMware Cloud Director is available through the token exchange flow that is detailed below. This flow does not involve the VMware Cloud Director UI and is suitable for scripted access, such as CLI.

1 Obtain a VMware Cloud Director JWT by either directly logging in or by using an API token.

2 Run a POST request.

```
POST  hostname/oidc/oauth2/token
```

   a Select `x-www-form-urlencoded` for the body of the request.

   b Include the following parameters in the body of the request.

```
{
     "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
     "assertion": "VMware_Cloud_Director JWT",
     "client_id": "Relying_party_ID",
     "scope": "openid profile email phone groups vcd_idp",
   }
```

3 The response returns both an ID token that includes the OIDC and VMware Cloud Director claims, and an access token that you can use to retrieve claims about the authenticated user at the *hostname*`/oidc/UserInfo` endpoint.

Encoded ID token example:

```
eyJhbGciOiJSUzI1NiIsInR5NDg4SI6I................4dHnbU1RQ6Y9Yohgw
```

Decoded ID token example:

```
{
  "at_hash": "1AA1aAA1AAAAAAaAA1A11a",
  "sub": "111111111-1111-1111-1111-11111111",
  "roles": [
    "Organization Administrator"
  ],
  "iss": "https://hostname/oidc",
  "groups": [
    "ALL USERS"
  ],
  "preferred_username": "testuser@vcd-ms1",
  "nonce": "ab123acab",
  "aud": "33333333-3333-3333-3333-33333333333",
  "azp": "22222222-2222-2222-2222-22222222",
  "org_id": "12345678-1234-1234-1234-123456789abc",
  "org_display_name": "oidcorg",
  "name": "test user",
  "phone_number": " ",
  "exp": 1111111111,
  "org_name": "oidcorg",
  "iat": 1111111111,
  "email": "user1@vmware.com"
}
```

User Info response example:

```
{
    "sub": "111111111-1111-1111-1111-11111111",
    "preferred_username": "administrator",
    "name": "administrator user",
    "email": "user1@site.com",
    "phone_number": "0 (111) 222-3333",
    "roles": [ "system administrator" ],
    "groups": [],
    "org_name": "system",
    "org_display_name": "System Organization",
    "org_id": "12345678-1234-1234-1234-123456789abc"
}
```

Multisite Considerations

In a multisite deployment, each site functions as a single identity provider server.

Paired sites do not provide federated identity server support. This means that if during the login process a tenant that does not belong to the site that functions as their identity provider proxy attempts to login to it through the organization selection of another site of the multisite deployment, login fails.

Configure VMware Cloud Director as an OpenID Provider Proxy Server

Starting with version 10.4.2, you can use VMware Cloud Director as a tenant-aware OpenId Connect (OIDC) identity provider proxy server.

After VMware Cloud Director is configured as an OIDC proxy server, when a user attempts to log in to the OIDC relying party (OIDC client), they are redirected to VMware Cloud Director and prompted to enter the name of their organization and their SSO or local credentials. After providing the necessary credentials, the user is directed to the OIDC relying party.

VMware Cloud Director delegates actual authentication to the authentication mechanism used by the provider or tenant. This can result in additional redirections to any external Identity Providers that perform authentication for those users.

Prerequisites

- Verify that your role includes the **OIDC Server: Manage Settings** right.
- Verify that the roles of the users that will log in to the OIDC relying party (OIDC client) through VMware Cloud Director include the **OIDC Server: Enable** right.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Settings**, click **OIDC Proxy**.

3 Click **Relying Parties** and click **New**.

4 Enter a relying party name for the client application registration and make a note of it.

5 Enter the URI to which to redirect users that are attempting to log in to the relying party, and click **Save**.

6 Copy the relying party ID and secret and make note of them.

7 Configure your OIDC relying party to use VMware Cloud Director as an identity provider proxy server with the relying party ID and secret.

   Tip You can retrieve the provider configuration values, including the JWKS endpoint and information about other endpoints and scopes necessary for the OIDC proxy configuration at the well-known configuration URL `*hostname*/oidc/.well-known/openid-configuration`. See View the OIDC Proxy General Settings in Your VMware Cloud Director.

Results

When a user attempts to log in to the OIDC relying party, they are redirected to VMware Cloud Director, prompted to select a VMware Cloud Director organization, and to provide their credentials. After a successful authorization, they are redirected back to the OIDC relying party.

View the OIDC Proxy General Settings in Your VMware Cloud Director

In the VMware Cloud Director **General Settings** tab, you can view the `openid-configuration` endpoint, from which you can retrieve the provider configuration values, indluding the JWKS endpoint and information about other endpoints and scopes necessary for the OIDC proxy configuration.

Prerequisites

Verify that your role includes the **OIDC Server: Manage Settings** right.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Settings**, click **OIDC Proxy**.

3 Click **General Settings**.

   The general OIDC proxy settings appear, including the well-known configuration URL from which you can retrieve the provider configuration values, the access token lifetime, the ID token lifetime, the authorization code lifetime and the redirect URL policy.

Managing OIDC Proxy Keys in Your VMware Cloud Director

When you configure VMware Cloud Director to function as an OIDC identity provider proxy, VMware Cloud Director generates a pair of OIDC keys with which it signs the JWT tokens that it issues.

When configured as an identity provider proxy server, VMware Cloud Director automatically generates a single built-in 2048-bit RSA signing key, which the **system administrator** can choose to use or to discard. Any new keys must comply with the minimum key size and the other VMware Cloud Director cryptographic requirements.

Tip To view the VMware Cloud Director key requirements, navigate to **Administration Settings > Settings > SSL**.

The relying parties that are using VMware Cloud Director as an OIDC proxy server can retrieve the provider configuration values, including the list of available public keys from the JWKS endpoint listed at `{{hostname}}/oidc/.well-known/openid-configuration`.

Prerequisites

Verify that your role includes the **OIDC Server: Manage Settings** right.

Add an OIDC Proxy Key Set Using Your VMware Cloud Director

You can manually add an OIDC proxy key set to VMware Cloud Director.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Settings**, click **OIDC Proxy**.

3 Click **Keys**.

4 To manually upload a new OIDC proxy key set, click **New**.

5 Enter a description for the OIDC proxy key.

  You can edit the key description later, if necessary.

6 Under Public Key, click **Browse Files**, navigate to the public key PEM file and upload it.

7 Under Private Key, click **Browse Files**, navigate to the private key PEM file and upload it.

8 Enter the private key passphrase.

9 Click **Save**.

Set a New OIDC Proxy Key Set As Active Using Your VMware Cloud Director

You can use the VMware Cloud Director UI to select a new active OIDC proxy key.

Prerequisites

- Verify that your role includes the **OIDC Server: Manage Settings** right.

- Verify that you uploaded the key set that you want to make active.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Settings**, click **OIDC Proxy**.

3 Click **Keys**

A list of the available key sets displays with the currently used key labeled as **Active**.

4 Select the new key set and click **Make Active**.

Delete an OIDC Proxy Key Set From Your VMware Cloud Director

If an OIDC key set is no longer in use, you can delete it.

Prerequisites

- Verify that your role includes the **OIDC Server: Manage Settings** right.

Procedure

1 In the top navigation bar, click **Administration**.

2 In the left panel, under **Settings**, click **OIDC Proxy**.

3 Click **Keys**

A list of the available key sets displays with the currently used key labeled as **Active**.

4 Select the key set that you want to remove, and click **Delete**.

Managing Certificates Using Your VMware Cloud Director

You can import, download, edit, and delete certificates from VMware Cloud Director. You can copy the certificate PEM data to the clipboard.

Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal

You can test the connection of VMware Cloud Director to a remote server, and establish a trust relationship with it.

You can test and secure the connection of VMware Cloud Director to a remote server by entering the server URL.

When you test a remote connection to a server, if the connection involves SSL communication and VMware Cloud Director hasn't already established a trust relationship with the server, you are prompted to review a certificate, or a chain of certificates, and to make a trust choice.

If the certificate chain is not complete and there are additional certificates available, you can choose to retrieve them to view more details before making a trust choice.

Prerequisites

Verify that your role includes the **SSL: Test Connection** and the **Truststore: Manage** rights.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Certificate Management**, select **Trusted Certificates** and click **Test Remote Connection**.

3 Enter an URL for the server with which you want to test the connection.

4 From the drop-down menu, select the hostname verification algorithm to use when testing the connection.

5 Click **Connect**.

6 If the connection involves SSL communication and VMware Cloud Director hasn't already established a trust relationship with the server, review the certificate information and make a trust choice.

Option	Description
Trust	Verify that you trust the certificate information and establish a trust relationship for future communication with the server.
Retrieve	If the certificate chain is not complete and there are additional intermediate and leaf certificates available from the same issuing certificate authority, you can retrieve them to view more details. Depending on your security considerations, choose one of the options. ■ Select which certificates to trust and click **Trust selected** ■ To cancel the attempt to establish a trust relationship, click **Cancel**
Cancel	Cancel the attempt to establish a trust relationship.

Import Trusted Certificates Using Your VMware Cloud Director Service Provider Admin Portal

You can import certificates of servers that VMware Cloud Director communicates with, such as vCenter Server, NSX-V Manager, and so on.

Note Instead of importing certificates manually, you can test the connection to the remote server and establish a trust relationship with it. See Test the VMware Cloud Director Connection to a Remote Server and Establish a Trust Relationship Using the Service Provider Admin Portal.

When using VMware Cloud Director in FIPS mode, you must use FIPS-compatible private keys. You can use pyOpenSSL to generate private keys in FIPS-compatible PKCS#8 format. If you generate PKCS#8 private keys by using OpenSSL, the private keys are not FIPS-compatible. For more information about FIPS mode, see Activate FIPS Mode on the Cells in the Server Group or Activate or Deactivate FIPS Mode on the VMware Cloud Director Appliance.

Prerequisites

Verify that your role includes the **Truststore: Manage** right.

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Certificate Management**, select **Trusted Certificates** and click **Import**.
3. Upload a PEM file containing the certificates that you want to import and click **Import**.
4. (Optional) Edit the certificate name.
5. Click **Import**.

What to do next

- Download a certificate.
- Edit a certificate name.
- Delete a certificate.
- Copy the PEM data to the clipboard.

Import Certificates to the Certificates Library Using Your VMware Cloud Director Service Provider Admin Portal

In the VMware Cloud Director certificates library, you can import certificates used when creating entities that you must secure, such as servers, edge gateways, and so on.

The certificate library contains information about single certificates, certificate chains, private keys, certificate expiration dates, the entities that the certificates secure, and so on.

You must manage the certificate libraries separately for each site.

When using VMware Cloud Director in FIPS mode, you must use FIPS-compatible self-signed certificates and private keys. You can generate self-signed unencrypted certificates and private keys by using OpenSSL. If you generate self-signed certificates and private keys by using OpenSSL, the certificates and private keys are not FIPS-compatible. For more information about FIPS mode, see Activate FIPS Mode on the Cells in the Server Group or Activate or Deactivate FIPS Mode on the VMware Cloud Director Appliance.

Prerequisites

- Verify that your role includes the **Certificate Library: Manage** right.
- Verify that the private keys you want to use are in the PKCS#8 format. VMware Cloud Director does not support private keys generated with the Digital Signature Algorithm (DSA).

Procedure

1. From the top navigation bar, select **Administration**.
2. In the left panel, under **Certificate Management**, select **Certificates Library** and click **Import**.

3. Enter a name, and optionally, a description for this certificate in the certificate library and click **Next**.
4. Upload a PEM file containing the certificate chain that you want to import and click **Next**.
5. (Optional) Upload a private key file.

   Your private key file might not be protected with a passphrase.
6. Click **Import**.

Results

The imported certificate appears in the list of available certificates during the creation of entities that you must secure.

What to do next

- Download a certificate.
- Edit the name and description of a certificate.
- Delete a certificate. You can delete only certificates that do not secure any entities.
- Copy the certificate PEM data to the clipboard.

Managing VMware Cloud Director Plug-Ins

VMware Cloud Director plug-ins expand the functions of the Service Provider Admin Portal and the VMware Cloud Director Tenant Portal. You can upload, deactivate, and delete plug-ins from the Service Provider Admin Portal. You can publish a plug-in to the service provider and individual organizations.

Some plug-ins are installed as part of VMware Cloud Director.

CPOM extension

Provides the capability for viewing and managing dedicated vCenter Server instances and proxies by using the VMware Cloud Director Tenant Portal.

Customize Portal

Provides the capability for customizing the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal.

VMware Cloud Director Availability

The VMware Cloud Director® Availability™ plug-in provides the capability to access VMware Cloud Director Availability Portal directly from the VMware Cloud Director user interface. For more information, see VMware Cloud Director Availability Documentation.

Guided Tours

Provides the capability to create and view guided tours of the VMware Cloud Director user interface. You can export the tours as shareable files.

vRO Workflow Execution UI

The vRO Workflow Execution UI plug-in provides the capability to import and run workflows that automate VMware Cloud Director processes.

Upload a Plug-in to Your VMware Cloud Director

You can upload additional plug-ins to your VMware Cloud Director Service Provider Admin Portal for use by the service provider and organizations in the cloud.

Prerequisites

Download the plug-in installation file.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Click **Upload**.

3 Click **Select plugin file**, browse to the target installation file, and click **Open**.

4 Click **Next**.

5 Select the scope for this plug-in.

Option	Description
Service Providers	The plug-in function becomes available in the VMware Cloud Director Service Provider Admin Portal.
Tenants	The plug-in function becomes available in the VMware Cloud Director Service Provider Admin Portal of the organizations that you select.

6 If you scoped the plug-in to tenants, select the organizations to which you want to publish this plug-in.

7 Review the **Review & Finish** page, and click **Finish**.

Activate or Deactivate a Plug-in Using Your VMware Cloud Director

To prevent all VMware Cloud Director organizations from using a plug-in, you can deactivate this plug-in.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the check box next to the names of the target plug-ins, and click **Enable** or **Disable**.

Delete a Plug-in From Your VMware Cloud Director

You can remove one or more plug-ins from the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the check boxes next to the names of the plug-ins that you want to remove, and click **Delete**.

3 To confirm, click **Save**.

Publish or Unpublish a Plug-in from a VMware Cloud Director Organization

You can modify the set of VMware Cloud Director organizations that can use the function provided by a plug-in.

You can modify the set of organizations for multiple plug-ins.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the check boxes next to the names of the target plug-ins, and click **Publish**.

3 Select the scope for this plug-in.

Option	Description
Service Providers	The plug-in function becomes available in the VMware Cloud Director Service Provider Admin Portal.
Tenants	The plug-in function becomes available in the VMware Cloud Director Service Provider Admin Portal of the organizations that you select.

4 If you scoped the plug-in to tenants, select the organizations to which you want to publish this plug-in.

5 Click **Save**.

Reinstall the VMware Hyper Plugin for VMware Cloud Director

If you delete the VMware Hyper Plugin for VMware Cloud Director, the **Customize Portal** page of the Service Provider Admin Portal becomes inaccessible. If you want to be able to install or manage any other plug-ins, you must reinstall the VMware Hyper Plugin.

Procedure

1 Download the VMware Hyper Plugin for the relevant VMware Cloud Director version on the Broadcom Support Portal.

Note Some versions of VMware Cloud Director support multiple versions of the VMware Hyper Plugin. You must install and enable all applicable versions of the VMware Hyper Plugin.

All applicable VMware Hyper Plugin versions are listed under the **Drivers and Tools** tab on the **Download VMware Cloud Director** page.

2 Manually upload the ZIP by using the VMware Cloud Director API.

The following steps use `SERVER` as the server endpoint of the VMware Cloud Director installation, and `TOKEN` as the `x-vcloud-authorization` header value that the initial session's creation request returns.

a Create a session using your **system administrator** credentials.

```
SERVER="vcloud.example.com" curl --header 'Accept: application/*+xml;version=30.0' --
insecure --basic --data '' --user 'administrator@System:pa$$w0rd' --verbose https://
$SERVER/api/sessions
```

b Using the `manifest.json` file as a template for the necessary values, register the plug-in.

```
SERVER="vcloud.example.com" TOKEN="c2f4258224ce4489b4e4474e4e34db15" curl --header
'Accept: application/json' --header 'Content-Type: application/json' --header
"x-vcloud-authorization: $TOKEN" --insecure --verbose https://$SERVER/cloudapi/
extensions/ui --data '{"pluginName": "Stub plugin", "vendor": "VMware", "description":
"", "version": "1.0.0", "license": "BSD-2", "link": "http://vcloud.example.com",
"provider_scoped": true, "enabled": true}'
```

c Enable file uploads for the plug-in.

You can find the endpoint information in the `Location` header of the previous response. The `size` is the size of the `plugin.zip` file in bytes.

```
SERVER="vcloud.example.com" TOKEN="c2f4258224ce4489b4e4474e4e34db15"
PLUGIN="urn:vcloud:uiPlugin:1e634a62-a98a-46c0-b9dd-7e2c5a9e8688" curl --header
'Accept: application/json' --header 'Content-Type: application/json' --header
"x-vcloud-authorization: $TOKEN" --insecure --verbose https://$SERVER/cloudapi/
extensions/ui/$PLUGIN/plugin --data '{"fileName": "plugin.zip", "size": 56623}'
```

d Upload the `plugin.zip` file to VMware Cloud Director.

You can find the upload path in the `Link` response header of the previous call.

```
SERVER="vcloud.example.com" TOKEN="c2f4258224ce4489b4e4474e4e34db15" curl --request
PUT --header 'Content-Type: application/zip' --header "x-vcloud-authorization: $TOKEN"
--insecure --verbose https://$SERVER/transfer/19d7fafd-6670-4c2a-983f-0b3a49725d2e/
plugin.zip --data-binary @dist/plugin.zip
```

3 If your VMware Cloud Director version supports more than one VMware Hyper Plugin version, repeat steps 1 and 2 for each supported VMware Hyper Plugin version.

Results

In the Service Provider Admin Portal, you can access the **Customize Portal** page, and the VMware Hyper Plugin for VMware Cloud Director appears in the list of plug-ins.

What to do next

To see the list of VMware Cloud Director plug-ins, from the top navigation bar, select **More > Customize Portal**.

Customizing the VMware Cloud Director Portals by Using the Legacy API

To match your corporate branding standards and to create a fully custom cloud experience, you can set the logo and the theme for your VMware Cloud Director Service Provider Admin Portal and for the VMware Cloud Director Tenant Portal of each organization. In addition, you can modify and add custom links to the two upper right menus in the VMware Cloud Director portals.

Starting with VMware Cloud Director 10.4, you can customize the VMware Cloud Director portals by using a new VMware Cloud Director API and UI. If you want to use the branding alpha feature, see Customizing the VMware Cloud Director Portals by Using the BrandingThemes API.

If you want to use the legacy VMware Cloud Director branding implementation, to customize your branding attributes and links, you must use the `branding` API endpoint. See Getting Started with VMware Cloud Director OpenAPI.

Portal Branding

As part of the installation, VMware Cloud Director contains two themes - default and dark. You can create, manage, and apply custom themes. In addition, you can change the portal name, the logo, and the browser icon. In addition, the browser title adopts the portal name that you set.

To customize the Service Provider Admin Portal, you must set the branding attributes at a system level. Unless you configure individual branding for a particular tenant, each organization adopts the system branding attributes.

For a particular tenant, you can selectively override any combination of the portal name, header color, logo, icon, theme, and custom links. Any value that you do not set uses the corresponding system default value.

Note By default, the individual tenant branding is not shown outside of a logged in session. The individual tenant branding does not appear on login and logout pages, so that tenants cannot discover the existence of other tenants. You can enable branding outside of logged in sessions by using the cell management tool:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

For information about using the cell management tool, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide* .

Custom Links

Custom links are a component of the portal branding. There are two types of custom links:

- `override` menu items replace the existing links for menu items **Help**, **About**, and **Download VMRC**. By default, **Download VMRC** redirects the users to https://my.vmware.com to download VMRC, which requires users to have registered accounts for downloading. By overriding this link, you can relocate the VMRC installer to your own server.
- `link` menu items are new links that you add to the user menu item in the upper-right corner of the portal where the **User preferences** and **Log out** options appear. The new custom links appear in the order given in the API call.

  You can organize these custom links by using the `section` and `separator` menu items. A `section` menu item adds a header to the menu, a `separator` menu item adds a line to the menu.

Custom links support custom placeholders which you can use to pass identifying information to other applications in the form of query parameters.

VMware Cloud Director supports the following custom variables in the `url` value for a custom link:

Table 11-2. Custom Variables for Custom Links

Variable	Description
`${TENANT_NAME}`	Organization name
`${TENANT_ID}`	Organization ID
`${SESSION_TOKEN}`	x-vcloud-authorization token

For example,

```
url: https://host:port/tenant/${TENANT_NAME}/vdcs
```

in the VMware Cloud Director Tenant Portal for organization myorg is converted to:

```
url: https://host:port/tenant/myorg/vdcs
```

Customizing the VMware Cloud Director Portals by Using the BrandingThemes API

To match your corporate branding standards and to create a fully custom cloud experience, customize the VMware Cloud Director portals by using the `BrandingThemes` API and corresponding UI. In addition, you can modify and add custom links to the two upper-right menus in the VMware Cloud Director portals, and to the login and logout pages.

Starting with VMware Cloud Director 10.4.1, you can customize the VMware Cloud Director portals by using a new VMware Cloud Director API and UI. The VMware Cloud Director UI provides a live preview of all changes so that you can see the modifications instantly without the need to save the theme. The `BrandingThemes` API and corresponding UI are an alpha feature, deactivated by default. To use it, you must activate it from the **Branding API** feature flag located under **Administration**. You can convert the existing legacy themes to the new theme format.

If you want to use the legacy VMware Cloud Director branding implementation, see Customizing the VMware Cloud Director Portals by Using the Legacy API.

Note By default, the individual tenant branding is not shown outside of a logged in session. The individual tenant branding does not appear on the login and logout pages, so that tenants cannot discover the existence of other tenants. You can enable branding outside of logged in sessions by using the cell management tool:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

For information about using the cell management tool, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Portal Branding

Unlike the legacy API, in the `BrandingThemes` API, the

As part of the installation, VMware Cloud Director contains two themes - light and dark. You can create, manage, and apply custom themes. In addition, you can change the portal name, the logo, the image on the login screen, and the browser icon. The browser title adopts the portal name that you set and login background.

When you create a theme, you can assign it to one or more tenant organizations. You can specify a theme to be the default theme, applicable to all organizations apart from the ones with specifically assigned themes through the **Assign** option.

For a particular theme, you can selectively override any combination of the portal name, colors, logo, icon, custom links, and login background. Any color value that you do not set uses the corresponding theme base color.

Certain operations are not applicable to some of the theme types.

Table 11-3. Theme operations

Theme type	Edit	Delete	Assign	Make default	Export	Clone
Built-in themes	-	-	✓	✓	✓	✓
Custom theme	✓	✓	✓	✓	✓	✓
Converted theme	-	✓	✓	✓	✓	✓
Assigned theme	✓	✓	✓	✓	✓	✓
Default theme	✓	-	-	-	✓	✓

Create a Custom VMware Cloud Director Portal Theme

To create a custom theme for the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal, you can use the Customize Portal plug-in.

When making any changes to the theme, you can instantly see how the selection would change the appearance of the theme.

Prerequisites

Verify that `BrandingThemes` API alpha feature is activated.

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Settings**, select the **Feature Flags** tab.

3 Select the **Branding API**, and click **Enable**.

4 For the changes to take effect, log out and log in again to the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the **Themes** tab.

3 From the **Create theme** drop-down menu, select a light-based or dark-based theme.

4 (Optional) Select the **Colors** tab, and select a color for each element of the theme.

5 Change the platform branding.

   a Select the **Branding** tab.

   b Enter a platform name.

      The platform name replaces the VMware Cloud Director name on the top navigation bar, the login page, and the browser title. If you want the theme to use the organization name at runtime, enter `${TENANT_NAME}` as a platform name.

   c Upload a platform logo.

      The platform logo replaces the VMware logo on the top navigation bar and the login page.

   d Upload a browser favicon.

      The favicon, or browser tab icon, is the icon that appears next to the page title in a browser tab.

   e Upload a background image for the login page.

      The login background image fills the full size of the screen and part of it is hidden below the login form. In addition, the image is centered and fills the screen entirely without distorting the image, changing width to height ratio, or leaving blank spots. Depending on the browser window size and screen resolution settings, some parts of the background image might not appear. Consider using a background with a pattern or an image that looks complete even if parts of it do not appear.

6 (Optional) In the **Links** tab, customize the platform links.

   a Enter new URLs for the **Help**, **About**, and **Download VM Remote Console** menu items.

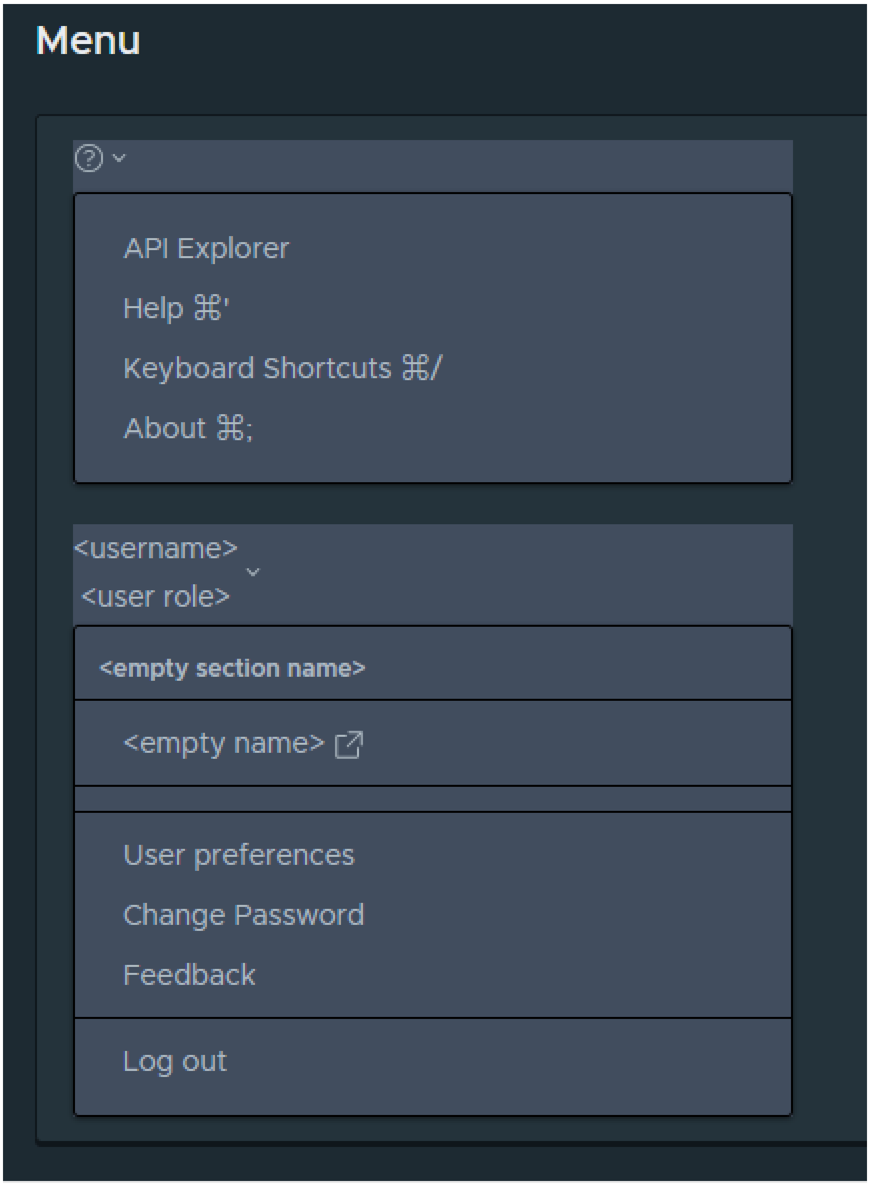
   The **Help** and **About** menu items are located in the **Help** menu on the right side of the top navigation bar. The **Download VM Remote Console** option is located in the **Actions > VM Console** menu of a VM.

   The **Override** items replace the existing links for the **Help**, **About**, and **Download VM Remote Console** menu items. By default, **Download VM Remote Console** redirects the users to https://my.vmware.com to download VMRC, which requires users to have registered accounts for downloading. By overriding this link, you can relocate the VMRC installer to your own server.

   b Create custom links, sections, and separators to the user menu.

   The **Menu** items are new links that you add to the user menu item in the upper-right corner of the portal. If you want the theme to automatically use the tenant name, tenant ID, or session token, use `${TENANT_NAME}`, `${TENANT_ID}`, or `${SESSION_TOKEN}` as placeholders.

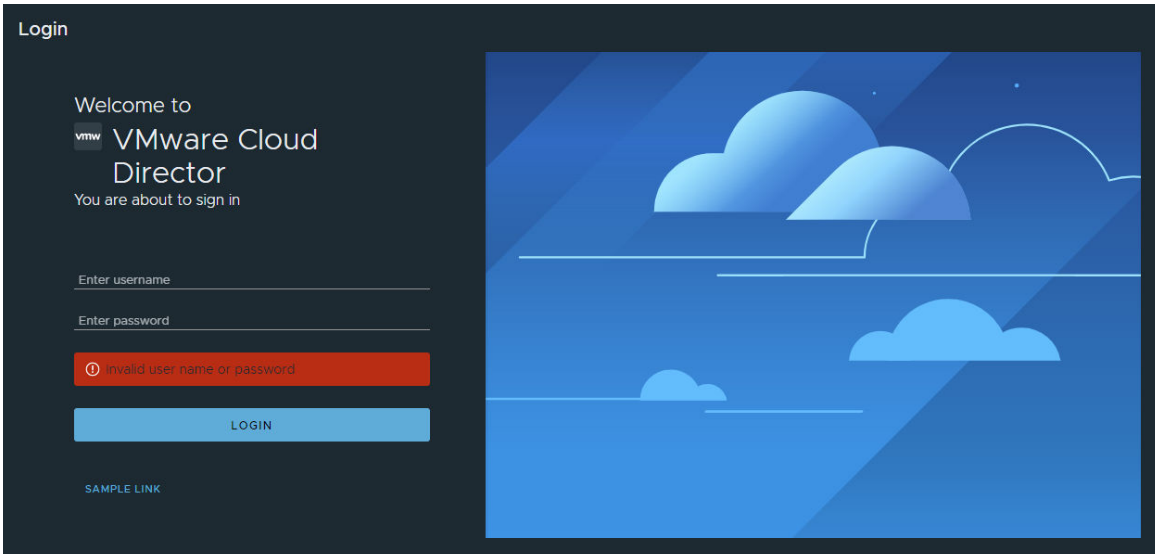
Variable	Description
`${TENANT_NAME}`	Organization name
`${TENANT_ID}`	Organization ID
`${SESSION_TOKEN}`	x-vcloud-authorization token



You can organize these custom links by selecting the **Section** and **Separator** menu items. A **Section** menu item adds a header to the menu, a **Separator** menu item adds a line to the menu.

c Add a link to the login page.

For example, you can add links to the terms and conditions on your platform, privacy and accessibility information, trademarks, and so on.



Login

Welcome to VMware Cloud Director

You are about to sign in

Invalid user name or password

d Add a link to the logout page.

For example, you can add links to the terms and conditions on your platform, privacy information, accessibility information, trademarks, and so on.

7 Click **Save**.

What to do next

From the **Actions** menu on the theme, you can make the theme a default one, assign the theme to an organization, export, clone, and delete the theme. You can assign to the Service Provider Admin Portal a theme different from the default theme. You can use the export option to clone a theme by importing it again to VMware Cloud Director.

The default theme changes affect all organizations apart from the ones with specifically assigned themes through the **Assign** option.

If an assigned theme becomes the default, it stops being explicitly assigned to organizations. When you change the default theme, VMware Cloud Director removes it from all organizations to which the theme was assigned to and replaces it with the new default.

Import a Custom VMware Cloud Director Portal Theme

You can export a custom portal theme from one VMware Cloud Director site and import it to another site.

Prerequisites

- Verify that you have an exported theme ZIP file. You can export an existing theme from its **Actions** menu.

- If you want to edit manually a ZIP file and use custom CSS for a theme, export the theme ZIP file and extract the file, make CSS changes to the theme, and compress the files to ZIP format again.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the **Themes** tab, and click **Import**.

3 Select a theme ZIP file, and click **Open**.

Results

The new theme appears on the **Customize Portal** page.

What to do next

From the **Actions** menu on the theme, you can make the theme a default one, assign the theme to an organization, export and delete the theme.

The default theme changes affect all organizations apart from the ones with specifically assigned themes through the **Assign** option.

If an assigned theme becomes the default, it stops being explicitly assigned to organizations. When you change the default theme, VMware Cloud Director removes it from all organizations to which the theme was assigned to and replaces it with the new default.

Convert a Legacy VMware Cloud Director Theme

You can convert themes modified through the legacy VMware Cloud Director branding implementation to themes that you can view and edit by using the VMware Cloud Director Service Provider Admin Portal or the new API endpoint.

Converted themes are read-only and marked as legacy. If you want to edit a converted theme, you must clone the theme and make changes to the clone. You can convert a legacy theme multiple times. You can identify the different conversions by the time stamp in their names.

Prerequisites

Verify that you have at least one theme modified through the legacy VMware Cloud Director branding implementation.

Procedure

1 From the top navigation bar, select **More > Customize Portal**.

2 Select the **Themes** tab, and click **Convert Old Themes**.

VMware Cloud Director detects if there are any themes that can be converted to the new format. If there are any legacy themes, VMware Cloud Director displays the applicable themes.

3 If you want to apply to the converted themes any pre-existing assignments to specific organizations, click **Apply assignments from the old themes**.

4 Click **Convert** and when the conversion is complete, click **Close**.

Configure the VMware Cloud Director Password Policy

To prevent a user from logging in to VMware Cloud Director after a certain number of failed attempts, you can enable the account lockout.

Changes to the system account lockout policy apply to all new organizations. Organizations created before the account lockout policy change must be changed at the organization level.

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Settings**, click **Password Policy**.

3 Click **Edit**.

4 To enable the account lockout, turn on the **Account lockout** toggle.

5 Select the accepted number of invalid logins before locking an account.

6 Select the lockout interval.

7 To enable the **system administrator** account lockout, turn on the **System Administrator account can be locked out** toggle.

8 Click **Save**.

Auto Scale Groups in Your VMware Cloud Director

You can allow VMware Cloud Director tenant users to auto scale applications depending on the current CPU and memory use.

Depending on predefined criteria for the CPU and memory use, tenants can use VMware Cloud Director to automatically scale up or down the number of VMs in a selected scale group. To allow tenants to auto scale applications, you must configure, publish, and grant access to the auto scale solution.

To balance the load of the servers that you configure to run the same application, you can use VMware NSX Advanced Load Balancer (Avi Networks).

Configure and Publish the Auto Scale Plug-in to Your VMware Cloud Director

Before granting access to tenants, you must configure the auto scale groups solution.

For multi-cell environments, you can run the commands on a single cell. VMware Cloud Director stores the configuration in the database which all other cells can use.

1 Log in directly or by using an SSH client to the OS of any of the cells in the cluster as **root**.

2 To enable metric data collection, choose between collecting data with or without metrics data persistence.

   - To collect metrics with metrics data persistence, set up the metrics collection in a Cassandra database. See *Install and Configure a Cassandra Database for Storing Historic Metroc Data* in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.
   - To collect metrics data without data persistence, run the following commands:

     ```
     $VCLOUD_HOME/bin/cell-management-tool manage-config -n
     statsFeeder.metrics.collect.only -v true
     ```

     Note Configuring a Cassandra database is not necessary for this option.

3 Enable the publishing of metrics.

   ```
   $VCLOUD_HOME/bin/cell-management-tool manage-config -n
   statsFeeder.metrics.publishing.enabled -v true
   ```

4 Create a `metrics.groovy` file in the `/tmp` folder with the following contents.

   ```
   configuration {
       metric("cpu.ready.summation") {
           currentInterval=20
           historicInterval=20
           entity="VM"
           instance=""
           minReportingInterval=300
           aggregator="AVERAGE"
       }
   }
   ```

5 Import the file.

   ```
   $VCLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
   metrics.groovy
   ```

6 If you configured Cassandra in step 2, update the Cassandra schema by providing the correct nodes addresses, database authentication details, port and metrics time to live in days.

   ```
   $VCLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
   nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
   TTL_days -update-schema
   ```

7 Enable auto scaling.

   a Create an auto scale system user.

b To configure the auto scale function, use the user name from step 7a.

```
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<user_name>
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>
```

When running the command from the terminal, escape any special characters using the backslash (\) sign.

8 If your environment is for development or testing purposes and you run the cell with self-signed certificates, run the following command.

```
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set
enableHostnameVerification=false
```

9 Restart the cell.

```
service vmware-vcd restart
```

10 Publish the Auto Scale Rights Bundle to Tenants in VMware Cloud Director

Publish the Auto Scale Rights Bundle to Tenants in VMware Cloud Director

If you want tenants to auto scale applications, you must publish the rights bundle to one or more organizations in your system. You can use auto scaling starting from VMware Cloud Director 10.2.2.

Prerequisites

Configure and Publish the Auto Scale Plug-in to Your VMware Cloud Director

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Verify that there are no **Legacy Rights Bundles** for the tenant organizations to which you want to grant access to auto scaling.

4 Select the **vmware:scalegroup Entitlement** bundle, and click **Publish**.

5. To publish the bundle:
   1. Select **Publish to Tenants**.
   2. Select the organizations to which you want to publish the role.
      - If you want to publish the bundle to all existing and newly created organizations in your system, select **Publish to All Tenants**.
      - If you want to publish the bundle to particular organizations in your system, select the organizations individually.
6. Click **Save**.

What to do next

Add the necessary **VMWARE:SCALEGROUP** rights to the tenant roles that you want to use scale groups. See View and Edit a Global Tenant Role Using Your VMware Cloud Director.

Monitoring VMware Cloud Director

12

System administrators can monitor completed and in-progress operations and view resource usage information at the provider virtual data center, organization virtual data center, and datastore level.

Starting with version 9.1, VMware Cloud Director does not support VMware vCenter Chargeback Manager. See the VMware Product Interoperability Matrices.

Read the following topics next:

- Generate and View the VMware Cloud Director Logs
- Configure Logging for the VMware Cloud Director Cells
- VMware Cloud Director and Cost Reporting
- View Use Information for a VMware Cloud Director Provider Virtual Data Center

Generate and View the VMware Cloud Director Logs

VMware Cloud Director provides logging information for each cloud cell in your server group. You can view the logs to monitor your cells and to troubleshoot any problems that you encounter during the day-to-day running of VMware Cloud Director.

To generate the logs, log in directly or by using an SSH client to the VMware Cloud Director server as **root**, and enter the following shortcut.

```
generate_support_bundle
```

VMware Cloud Director Logs

Log Name File or Directory	Description
`/opt/vmware/vcloud-director/logs/cell.log`	Console output from the VMware Cloud Director cell.
`/opt/vmware/vcloud-director/logs/cell-management-tool`	Cell management tool log messages from the cell.
`/opt/vmware/vcloud-director/logs/cell-runtime`	Runtime log messages from the cell.
`/opt/vmware/vcloud-director/logs/cloud-proxy`	Cloud proxy log messages from the cell.

Log Name File or Directory	Description
`/opt/vmware/vcloud-director/logs/server-group-communications`	Server group communications from the cell.
`/opt/vmware/vcloud-director/logs/statsfeeder`	Virtual machine metric retrieval from vCenter Server and storage information and error messages.
`/opt/vmware/vcloud-director/logs/vcloud-container-debug.log`	Debug-level log messages from the cell.
`/opt/vmware/vcloud-director/logs/vcloud-container-info.log`	Informational log messages from the cell. This log also shows warnings or errors encountered by the cell.
`/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log`	Informational log messages from the cell watchdog. It records when the cell stops responding, is restarted, and so on.
`/opt/vmware/vcloud-director/logs/diagnostics.log`	Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.
`/opt/vmware/vcloud-director/logs/`*YYYY_MM_DD*`.request.log`	HTTP request logs in the Apache common log format.
`opt/vmware/vcloud-director/logs/vclistener.log`	The VCListener includes the Property collector reader that collects data from vCenter Server and the PCEventProcessors that asynchronously process the updates received from vCenter Server. This log includes all the log statements corresponding to these components.
`/opt/vmware/vcloud-director/logs/activityevent.log`	For each completed event, a list of local users must receive a completion event from other cells through message bus. You can use the `activityevent.log` to identify whether there is a completion event in the log.
`/opt/vmware/vcloud-director/logs/jobscheduler.log`	You can use the log to identify issues regarding periodical scheduled activities running in VMware Cloud Director.

VMware Cloud Director Appliance Logs

The VMware Cloud Director appliance features some additional log files.

Log file	Description
`/opt/vmware/var/log/firstboot`	Contains logging information related to the first boot of the appliance.
`/opt/vmware/var/log/vcd`	Contains logs related to the Replication Manager (`repmgr`) tool suite setup, reconfiguration, and appliance synchronization.
`/opt/vmware/var/log/vcd/pg`	Contains logs related to the backup of the embedded appliance database.
`/opt/vmware/etc/vami/ovfEnv.xml`	Contains the OVF deployment parameters.

Log file	Description
`/var/vmware/vpostgres/current/pgdata/log`	Contains logs related to the embedded PostgreSQL database.
`/opt/vmware/var/log/vami/updatecli.log`	Contains logging related to appliance upgrades.

Use any text editor, text viewer, or third-party tool to view the logs.

Configure Logging for the VMware Cloud Director Cells

VMware Cloud Director has different logging levels. The default logging configuration might not be sufficient for busy environments or for capturing events whilst troubleshooting. You might need to change the level of logging and even the sizes and number of files retained.

Important Verify that you are aware of the consequences to your VMware Cloud Director server group when making changes to the log configuration without guidance from the VMware Global Support team. If you change a logging level to a more verbose one, the logs might start to expand very fast, and your VMware Cloud Director environment might run out of disk space.

The VMware Cloud Director logs are located in the `/opt/vmware/vcloud-director/logs/` directory.

The VMware Cloud Director log configuration file is located in the `/opt/vmware/vcloud-director/etc/` directory. The name of the log configuration file is `log4j.properties`.

If you customize the `log4j.properties` log configuration file, before a VMware Cloud Director upgrade, you must make a copy of the `log4j.properties`, and after the upgrade, manually insert any missing sections.

To improve your log retention and to ensure that the VMware Cloud Director logs are kept for a certain amount of time, consider using a syslog server.

Table 12-1. Logging Levels

Logging Level	Description
`FATAL`	`FATAL` is the least verbose level. This level logs very severe error events that might cause the application to fail.
`ERROR`	This level logs error events that might still allow the application to continue running.
`WARN`	This level logs potentially harmful situations and warnings.
`INFO`	This level logs informational messages that highlight the progress of the application at a coarse-grained level.

Table 12-1. Logging Levels (continued)

Logging Level	Description
`DEBUG`	This level logs informational events that are most useful to debug an application at a fine-grained level.
`TRACE`	`TRACE` is the most verbose level. This level logs informational events at a more fine-grained level than the `DEBUG` level logging.

Prerequisites

Make a backup copy of the `/opt/vmware/vcloud-director/etc/log4j.properties` file.

Consider

Procedure

1 Log in directly or by using an SSH client to the VMware Cloud Director console as **root**.

2 Open the `/opt/vmware/vcloud-director/etc/log4j.properties` file in a text editor.

3 Locate the `Default vCloud loggers` section, and modify the log level for the loggers.

The following example shows the log level set to the most verbose level.

```
log4j.logger.com.vmware.vcloud=TRACE
log4j.logger.com.vmware.ssdc=TRACE
```

4 Locate the log file definition that you want to update.

```
log4j.appender.Feature.File=logs/File_Name
```

For example, you might want to change the logging level for the `# Component appender for container debug` section. The last line of the section configures the level of logging that the file captures.

5 Set the logging level to the value you want.

Important Verify that you are aware of the consequences to your VMware Cloud Director server group when making changes to the log configuration without guidance from the VMware Global Support team.

The following example changes the line to match the most verbose level.

```
log4j.appender.vcloud.system.debug.threshold=TRACE
```

6 If you change the recording to a more verbose level, you might need to increase the number of log backups and the size of the log files.

   a Locate the `MaxFileSize` and `MaxBackupIndex` lines.

   ```
   log4j.appender.vcloud.system.debug.MaxFileSize=
   ```

   ```
   log4j.appender.vcloud.system.debug.MaxBackupIndex=
   ```

   b Change the default settings.

   For example, if you want the log files to expand to 50 MB before they rollover and to keep the last 18 logs, change the lines as follows.

   ```
   log4j.appender.vcloud.system.debug.MaxFileSize=50000KB
   ```

   ```
   log4j.appender.vcloud.system.debug.MaxBackupIndex=18
   ```

   When a file reaches the selected 50 MB size, VMware Cloud Director continues to log data in a new file and keeps up to 18 backups.

Important If you change a logging level to a more verbose one, the logs might start to expand very fast, and your VMware Cloud Director environment might run out of disk space.

7 Save the `/opt/vmware/vcloud-director/etc/log4j.properties` file.

VMware Cloud Director applies the changes immediately. The `Log4J.properties` file does not have explicit lines for changing the size and amount of logs that VMware Cloud Director keeps.

Control the API Request Logging in VMware Cloud Director

You can control the process of capturing and storing information about incoming requests in VMware Cloud Director.

VMware Cloud Director logs the incoming requests to the VMware Cloud Director cells in request logs. The logs have names of the form *`YYYY_MM_DD`*`.request.log`. You can find the VMware Cloud Director `request.log` files in the `/opt/vmware/vcloud-director/logs/` directory, but you cannot configure the logs through the `log4j.properties` file.

You can use the `manage-config` subcommand of the command line tool to control the API request logging. The `manage-config` subcommand changes the settings for the whole server group. For more information about the `manage-config` subcommand options and arguments, see Updating Application Configuration Settings in VMware Cloud Director.

The log rotation can happen maximum once per day and is not linked to the size of the individual log files or the total size of all log files. You can control the rotation policy by changing the amount of days for which VMware Cloud Director keeps the logs.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director cell as **root**.

2 If you want change the retention policy of the request logs, use the `manage-config` subcommand of the cell management tool.

  The retention policy value represents the number of days for which VMware Cloud Director retains the National Center for Supercomputing Applications (NCSA) compliant request log. The default value is `0`, where `0` means forever. Deleting the value also keeps the logs forever. The least amount of time you can keep the logs is 1 day.

  ```
  /opt/vmware/vcloud-director/bin/cell-management-tool manage-config --name
  "vcloud.http.log.retainDays" --value New_Value
  ```

3 For the changes to take effect, you must restart the cells.

  After you restart a cell, it begins using the updated value. You can restart part of the cells or all of the cells at once.

VMware Cloud Director and Cost Reporting

You can use VMware vRealize Operations Tenant App for VMware Cloud Director to configure a cost reporting system for VMware Cloud Director.

The VMware vRealize Operations Tenant App features metering capabilities that allow service providers to provide their customer base with chargeback services.

The VMware vRealize Operations Tenant App is also a tenant facing application which provides tenant administrators with visibility to their environment and to their billing data.

For information about compatibility between VMware Cloud Director and VMware vRealize Operations Tenant App, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

You can download the VMware vRealize Operations Tenant App at https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director.

For information on how to use the VMware vRealize Operations Tenant App, see *Using vRealize Operations Tenant App for VMware Cloud Director as a Service Provider* and *Using vRealize Operations Tenant App for VMware Cloud Director as a Tenant*.

View Use Information for a VMware Cloud Director Provider Virtual Data Center

Provider virtual data centers provide compute, memory, and storage resources to its VMware Cloud Director organization virtual data centers. You can monitor the use of the provider virtual data center resources, so that you can decide to add more resources.

Procedure

1. From the top navigation bar, select **Resources** and click **Cloud Resources**.
2. In the left panel, select **Provider VDCs**, and click the name of the target provider virtual data center.
3. Click the **Configure > Metrics**tab.
4. For details about each parameter, click each information icon.

Managing Services in VMware Cloud Director

13

The Content Libraries view in the VMware Cloud Director Service Provider Admin Portal provides an interface for the integration with VMware Aria Automation Orchestrator. The VMware Aria Automation Orchestrator workflows are available as a catalog of services that service provider administrators can publish to tenants or other service providers and in this way extend the set of functionalities and management capabilities they offer.

Read the following topics next:

- Integrating VMware Aria Automation Orchestrator with VMware Cloud Director
- Create a Service Category Using Your VMware Cloud Director
- Edit a Service Category Using Your VMware Cloud Director
- Import a Service to Your VMware Cloud Director
- Search for a Service in Your VMware Cloud Director
- Execute a Service Using Your VMware Cloud Director
- Change a Service Category Using Your VMware Cloud Director
- Unregister a Service From VMware Cloud Director
- Publish a Service to Your VMware Cloud Director

Integrating VMware Aria Automation Orchestrator with VMware Cloud Director

You integrate VMware Aria Automation Orchestrator with VMware Cloud Director through the VMware Cloud Director Service Provider Admin Portal.

Integrating VMware Aria Automation Orchestrator with VMware Cloud Director extends the base functionality of VMware Cloud Director by allowing service provider administrators to develop complex automation tasks through workflow orchestration and utilization of third-party plug-ins.

Through the VMware Cloud Director Service Provider Admin Portal, service provider administrators are able to view, import, and execute workflows from registered VMware Aria Automation Orchestrator server instances.

In the VMware Cloud Director Service Provider Admin Portal, VMware Aria Automation Orchestrator workflows can be published to service providers or tenants, allowing for quick access control and execution of both custom and built-in services.

VMware Aria Automation Orchestrator has an extensive workflow library that contains pre-built tasks designed to solve specific challenges and perform common administrative tasks. Third-party plug-ins are also available at VMware Solution Exchange.

Starting with VMware Cloud Director 10.3, a vRO Workflow Execution UI plug-in is installed as part of VMware Cloud Director. The plug-in is enabled and published by default for service providers. To enable the plug-in for use by tenants, a **system administrator** must publish it to either a single tenant or to all tenants. For more information, see Managing VMware Cloud Director Plug-Ins.

Register a VMware Aria Automation Orchestrator Instance with VMware Cloud Director

To leverage orchestration of workflows and automation of tasks through VMware Aria Automation Orchestrator in VMware Cloud Director, you register a VMware Aria Automation Orchestrator instance in the VMware Cloud Director Service Provider Admin Portal.

Prerequisites

- Deploy and configure a VMware Aria Automation Orchestrator server instance. For more information, see *Installing and Configuring VMware Aria Automation Orchestrator* in the VMware Aria Automation Orchestrator documentation.
- Configure VMware Aria Automation Orchestrator to use vSphere as an authentication provider.
- Verify that you enabled the vRO Workflow Execution UI plug-in. See Managing VMware Cloud Director Plug-Ins.
- To secure the communication with the VMware Aria Automation Orchestrator server instance, import its certificate to VMware Cloud Director. See Managing Certificates Using Your VMware Cloud Director.

Procedure

1 From the top navigation bar, select **Libraries**

   a From the left panel, select **Service Management**.

   A list of registered VMware Aria Automation Orchestrator server appears.

2 To register a new VMware Aria Automation Orchestrator server, click **Add**.

   The **Register vRealize Orchestrator** dialog appears.

3 Enter the following values.

Option	Description
Name	Name for the registered VMware Aria Automation Orchestrator instance.
Description	Description for the registered VMware Aria Automation Orchestrator server instance.
Hostname	The fully-qualified domain name and server port of the VMware Aria Automation Orchestrator server. The default HTTPS port value is 443. **Note** VMware Cloud Director connects to the API interface of VMware Aria Automation Orchestrator.
Username	A user account that is member of the VMware Aria Automation Orchestrator administrators group.
Password	The password for the VMware Aria Automation Orchestrator administrator account.
Choose vRO vCenter	Choose one of the following. ■ From the drop-down menu, select the vCenter Server instance that is backing the VMware Aria Automation Orchestrator server instance. ■ If there is more than one vCenter Server instance, to automatically add the vCenter Server instance that backs VMware Aria Automation Orchestrator, click **Auto Discover**.

4 Click **OK** to complete the registration.

Create a Service Category Using Your VMware Cloud Director

You can organize services in service categories.

Procedure

1 From the top navigation bar, select **Libraries**

a From the left panel, select **Service Management**.

b Navigate to the **Service Categories** tab.

A list of existing server categories appears.

2 To create a new service category, click **Add**.

The **New Service Category** dialog appears.

3 Enter the following values.

Option	Description
Name	Name of the service category.
Icon	Import the displayed icon for the service category.
Description	Short description of the service category.

Edit a Service Category Using Your VMware Cloud Director

You can edit existing service categories.

Procedure

1 From the top navigation bar, select **Libraries**

   a From the left panel, select **Service Management**.

   b Navigate to the **Service Categories** tab.

   A list of existing server categories appears.

2 Use the list bar (⋮) on the left of a selected service category and click **Edit**.

3 Edit the following values.

Option	Description
Name	Name of the service category.
Icon	Import the displayed icon for the service category.
Description	Short description of the service category.

Import a Service to Your VMware Cloud Director

You can import services from the workflow library of a VMware Aria Automation Orchestrator instance that is registered with VMware Cloud Director.

Prerequisites

- Register a VMware Aria Automation Orchestrator instance. See Register a VMware Aria Automation Orchestrator Instance with VMware Cloud Director.
- Create a service category. See Create a Service Category Using Your VMware Cloud Director.
- Verify that you enabled the vRO Workflow Execution UI plug-in. You can scope and publish the plug-in to the service provider and to individual tenants. See Managing VMware Cloud Director Plug-Ins.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, select **Service Library**.

   Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 To import a new service, click the **Import** button.

3 Follow the steps of the **Import** wizard.

Option	Description
Import to target library	Select the service category, to which to import the service.
Select source	Select the VMware Aria Automation Orchestrator instance, from which to import workflows.
Select workflows	Expand the hierarchical tree view to select one or multiple workflows to import.
Review	Review the details and click **Done** to complete the import.

The imported workflows appear in the **Service Library c**ard view.

Search for a Service in Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can search for a service by its name or the service category it belongs to.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, select **Service Library**.

   Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 In the **Search** text box on the top of the page, enter a word or a character of the name of the service or the service category you want to find.

   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 Using Your VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, you can execute VMware Aria Automation Orchestrator workflows as imported services.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, select **Service Library**.

   Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 To execute a service, in the card of the selected service, click **Execute**.

The **Execute a service** wizard appears.

3 Fill in the required input parameters of the service and click **Finish**.

Results

You can monitor the status of the execution in the **Recent Tasks** view. For more information, see View Tasks in Your VMware Cloud Director Service Provider Admin Portal.

Note When you start a VMware Aria Automation Orchestrator workflow as a VMware Cloud Director service, VMware Cloud Director adds a few custom parameters to the workflow execution context.

Custom Property	Description
`_vcd_orgName`	Name of the organization, to which the user who executes the service belongs.
`_vcd_orgId`	ID of organization, to which the user who executes the service belongs.
`_vcd_userName`	Name of the user who executes the service.
`_vcd_isAdmin`	Has value `True` if the user who executes the service is an **administrator**.
`_vdc_isAdmin`	Deprecated. Has value `True` if the user who executes the service is an **administrator**.
`_vdc_userName`	Deprecated. Name of the user who executes the service.
`_vcd_sessionToken`	Authentication token you received after successful authentication to VMware Cloud Director
`_vcd_apiEndpoint`	VMware Cloud Director REST API endpoint

Change a Service Category Using Your VMware Cloud Director

In VMware Cloud Director Service Provider Admin Portal, you can change the category, to which a service belongs.

Procedure

1 From the top navigation bar, select **Libraries**.

a From the left panel, select **Service Library**.

Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 In the card of the selected service, select **Manage > Change Category**.

The **Change Category** dialog opens.

3 Select the category in which to place the service and click **Save**.

Unregister a Service From VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can remove access to a service for both service providers and tenants by unregistering the service.

Procedure

1 From the top navigation bar, select **Libraries**.

  a From the left panel, select **Service Library**.

  Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 In the card of the selected service, select **Manage > Unregister Workflow**.

  The **Unregister Workflow** dialog opens.

3 To remove the service from the service library, click **Delete**.

Publish a Service to Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can control service provider and tenant access to services by publishing a service.

Procedure

1 From the top navigation bar, select **Libraries**.

  a From the left panel, select **Service Library**.

  Available services display in a card view of 12 items per page, sorted by names in alphabetical order. Each card indicates that the item is a VMware Aria Automation Orchestrator workflow and shows the name of the service and a tag that corresponds to the service category, in which the workflow is imported.

2 In the card of the selected service, select **Manage > Publish Workflow**.

  The **Publish Workflow** dialog box appears.

3 To publish to service providers, select **Publish to Service Providers** and click **Save**.

4 To publish to a specific tenant organization, select **Publish to Tenants** button.

  a A list with available tenant organizations appears. Select the tenant organization, to which to publish the workflow and click **Save**.

5 To publish to all tenant organizations, select **Publish to All Tenants** and click **Save**.

Managing Defined Entities in VMware Cloud Director 14

To create extensions that provide additional VMware Cloud Director capabilities to the tenants, service providers can use the VMware Cloud Director API.

Defined entities represent external resources that VMware Cloud Director can manage. Extension and UI plug-in developers can create runtime defined entities, enabling extensions and UI plug-ins to store and manipulate the extension-specific information in VMware Cloud Director. If you create an extension and it needs to store a state or references to external resources, the extension can use runtime defined entities instead of a local database. For example, a Kubernetes extension can store information about the Kubernetes clusters it manages in runtime defined entities. The extension can then provide extension APIs for managing those clusters using the information from the runtime defined entities.

You can access runtime defined entities only through the VMware Cloud Director API. Users with admin privileges can track and observe the way extensions operate by verifying the state of the defined entities that the extensions create. The states of the defined entities can also help you to troubleshoot problems with the extensions.

Defined Entity Type

You define at runtime the schema of the information that you can store by using defined entities. The schema is defined in the entity type through a JSON document. When you create a defined entity type, you create a new custom VMware Cloud Director type similar to VMs and vApps which you can manage by extensions and behaviors. For example, if we consider the entity type `NativeContainerCluster`, each instance of this type contains information about a specific Kubernetes cluster. To obtain the information about the cluster, the VMware Cloud Director Container Service Extension communicates with VMware Cloud Director through the VMware Cloud Director API and provides the necessary information to the users.

Once you create an instance of a defined entity type, you cannot change the type, schema, and behaviors anymore. To add new functionalities to the entity type, you must create a new version of the type. When a defined entity instance is based on an earlier version of the entity type, you can upgrade the defined entity to use a later version of the type by setting the type property of the entity to the ID of the new type. When you create a defined entity, in the API call, the contents of the entity property must match the JSON schema specified in the entity type. You can grant access to an entity type only to specific users and organizations. You can set different access restrictions to the different versions of an entity type.

The schema of the entity type can specify the access to the different content fields. You can mark properties as `public`, `protected`, or `private`.

Table 14-1. Entity Type Property Access Control

Property Status	Access Control
`Public`	All users can view and modify the field.
`Protected`	All users can view the field. Only users with Full Control access can create and modify the field. The users must have the Admin Full Control: TYPE right or both the Full Control: TYPE right and a Full Control ACL.
`Private`	Only users with Full Control access can view, create, and modify the field. The users must have the Admin Full Control: TYPE right or both the Full Control: TYPE right and a Full Control ACL

For example, the JSON schema for the entity property `clusterState` can be the following.

```
"clusterState" : {
  "type" : "string",
  "x-vcloud-restricted" : "protected"
}
```

Interfaces and Behaviors

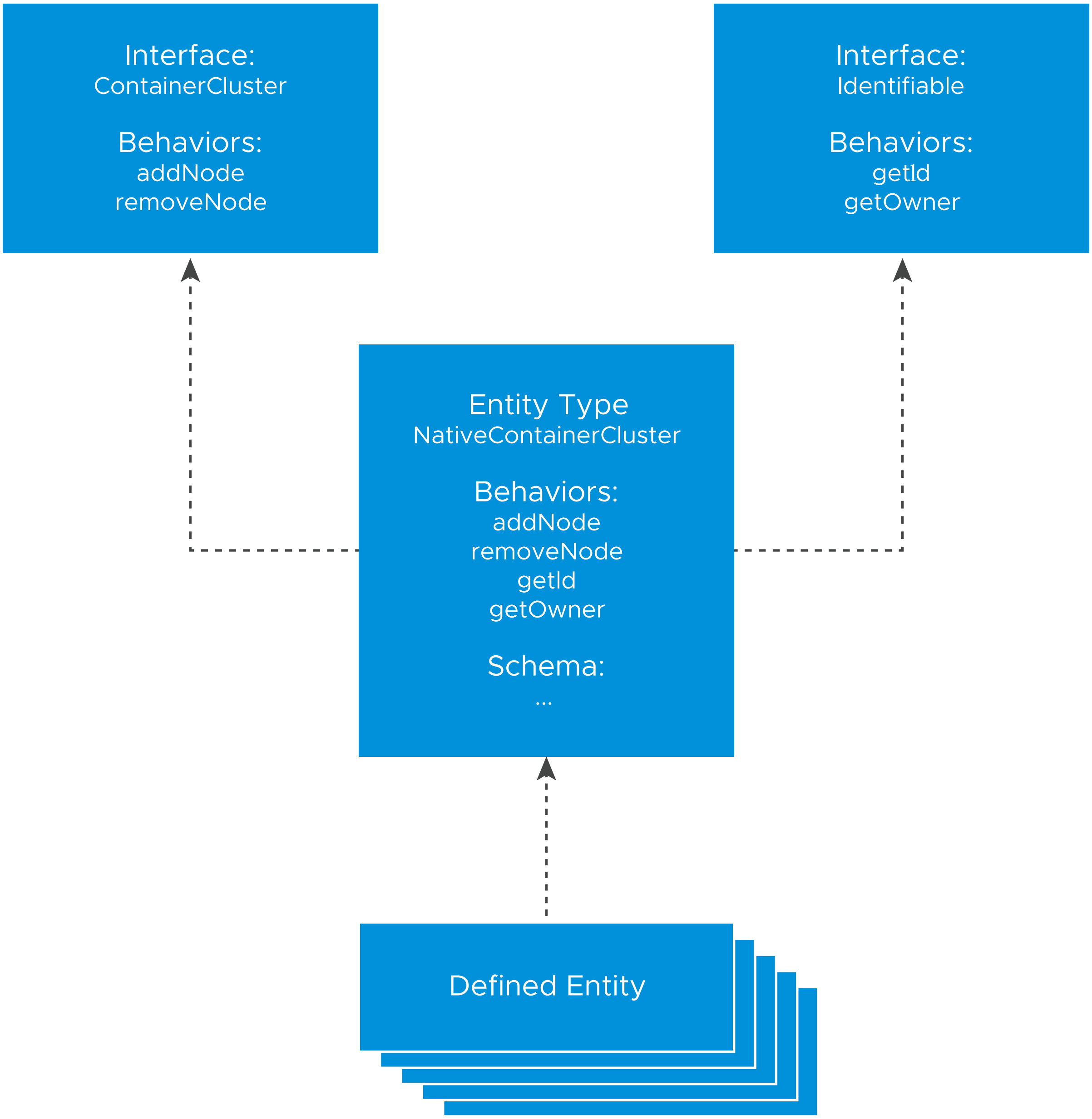
Defined entities also have interfaces that you can use to define behaviors. If we use the Kubernetes example, each cluster entity type has a different implementation of the behaviors defined in the container cluster interface. The Tanzu Kubernetes cluster type behaviors communicate with vSphere to perform the necessary actions and the native container cluster type behaviors communicate with the VMware Cloud Director Container Service Extension.

All users can see the interfaces of defined entities.

There are different ways to define behaviors.

- You can create and publish a VMware Aria Automation Orchestrator workflow and create a behavior that invokes the workflow.
- You can link any functionality to a behavior by using a WebHook.
- With MQTT behaviors, you can call a functionality in an extension. By using MQTT you can communicate with the extension directly and the extension can provide a more detailed status.

Figure 14-1. Runtime Defined Entity Interfaces



Runtime defined entity interfaces, types, and behaviors have specific API IDs.

- Interface API IDs are in the form of `urn:vcloud:interface:`*`vendor_name`*`:`*`interface_name`*`:`*`version`*.
- Type API IDs are in the form of `urn:vcloud:type:`*`vendor_name`*`:`*`type_name`*`:`*`version`*.
- Behavior API IDs are in the form of `urn:vcloud:behavior-interface:`*`behavior_name`*`:`*`vendor_name`*`:`*`interface_name`*`:`*`version`* or `urn:vcloud:behavior-type:`*`behavior_name`*`:`*`vendor_name`*`:`*`interface_name`*`:`*`version`*.

Creating a Runtime Defined Entity

To create a defined entity, you start by configuring the external resources and adding the necessary information to the defined entity. This process might require a few iterations. To resolve the defined entity, you must verify that the contents of the schema have all the necessary information. If the contents do not match the JSON schema specified in the type, the defined entity state changes to `Resolution_Error`. If you fill in the information correctly, the defined entity state changes to `Resolved` and is ready to use.

Because tasks track all long-running runtime defined entity operations, you can use the VMware Cloud Director UI to monitor the creation of defined entities, behavior invocation, and so on. When the status of a defined entity changes to `Resolved`, the corresponding task in the UI appears as `Succeeded`.

When you create a defined entity in one tenant organization, you cannot share the defined entity with tenants in another organization. If you create a defined entity in the `System` organization, you can share it with tenant users or tenant organizations.

Sample API Call to Create a Defined Entity

The example provides a sample API call to create a new entity of the `pksContainerCluster` type.

```
POST https://host/cloudapi/1.0.0/entityTypes/urn:vcloud:type:vendorA:pksContainerCluster:1.0.0
{
   "name": "testEntity",
   "entity": {
      "cluster": {
         "name": "testCluster",
         "nodes": ["node1"]
      }
   }
}
```

Access to Defined Entity Instances

Two complementary mechanisms control the access to runtime defined entities.

- Rights - When you create a runtime defined entity type, you create a rights bundle for the type. To provide access to specific operations, you must assign rights from this bundle to other roles. Each bundle has five type-specific rights: **View: TYPE**, **Edit: TYPE**, **Full Control: TYPE**, **Administrator View: TYPE**, and **Administrator Full Control: TYPE**.

  The **View: TYPE**, **Edit: TYPE**, and **Full Control: TYPE** rights work only in combination with an ACL entry.

- Access Control List (ACL) - The ACL table contains entries defining the access users have to specific entities in the system. It provides an extra level of control over the entities. For example, while an **Edit: TYPE** right specifies that a user can modify entities to which they have access, the ACL table defines which entities the user has access to.

System administrators with the **View General ACL** right can view the ACLs assigned to a specific defined entity by using the `accessControls` API. See VMware Cloud Director OpenAPI.

System administrators with the **Manage General ACL** right can create, modify, and remove specific ACLs by using the `accessControls` API.

Table 14-2. Rights and ACL Entries for RDE Operations

Entity Operation	Option	Description
Read	**Administrator View: TYPE** right	Users with this right can see all runtime defined entities of this type within an organization.
	View: TYPE right and ACL entry **>= View**	Users with this right and a read-level ACL can view runtime defined entities of this type.
Modify	**Administrator Full Control: TYPE** right	Users with this right can create, view, modify, and delete runtime defined entities of this type in all organizations.
	Edit: TYPE right and ACL entry **>= Change**	Users with this right and modify-level ACL can create, view, and modify runtime defined entities of this type.
Delete	**Administrator Full Control: TYPE** right	Users with this right can create, view, modify, and delete runtime defined entities of this type in all organizations.
	Full Control: TYPE right and ACL entry **= Full Control**	Users with this right and full control-level ACL can create, view, modify, and delete runtime defined entities of this type.

You can use the VMware Cloud Director API or UI to publish the rights bundle to any organizations you want to manage the entities of this type. After publishing the rights bundle, you can assign rights from the bundle to roles within the organization.

You can use the VMware Cloud Director API to edit the ACL table.

Access to Defined Entity Interface and Type Operations

Defined entity interface and type operations require specific rights that certain service providers might not have. Before performing an operation, verify that you have the necessary rights.

Table 14-3. Rights for Defined Entity Interface and Type Operations

Operation	Requirement
View and query interface	All users have the necessary rights.
Create interface	You must have the **Create new custom entity definition** right.
Edit interface	You must have the **Edit custom entity definition** right.
Delete interface	You must have the **Delete custom entity definition** right.
Create type	You must have the **Create new custom entity definition** right.
View type	The minimum requirement is `ReadOnly` Type ACL.
Edit and delete type	You must have the **Edit/Delete custom entity definition** right and a `FullControl` Type ACL .

Working with Runtime Defined Entities

To invoke behaviors on a defined entity, it must be in the `Resolved` state. To delete a defined entity, it must be in the `Resolved` or `Resolution_Error` state.

You can modify entity types and interfaces only if they do not have instances. You can only modify the referenced entity type by changing its version.

To diagnose issues with the access to defined entities,you can use the entity ACL query APIs and verify the necessary rights. In addition, the rights bundle of an entity type must be published to the tenants that you want to use it.

Read the following topics next:

- Sharing Defined Entities in VMware Cloud Director
- VMware Cloud Director Webhook Behaviors
- Managing Custom Entities in VMware Cloud Director

Sharing Defined Entities in VMware Cloud Director

You can grant access to Runtime Defined Entities (RDEs) by sharing them with other VMware Cloud Director system administrators or tenants.

Sharing Defined Entities with Another User

1 If you want to grant access to defined entities to tenants, publish the rights bundle of the defined entity type to a tenant organization. For example, for the creation and management of Tanzu Kubernetes clusters, you must publish the **vmware:tkgcluster Entitlement** rights bundle. See Publish or Unpublish a Rights Bundle to VMware Cloud Director.

  If you want to share the defined entity with a **system administrator**, skip this step.

2. Assign the **View: TYPE**, **Edit: TYPE**, or **Full Control: TYPE** right from the bundle to the user roles you want to have the specific level of access to the defined entity.

   For example, if you want the users with the **tkg_viewer** role to view Tanzu Kubernetes clusters within the organization, you must add the **View: Tanzu Kubernetes Guest Cluster** right to the role. If you want the users with the **tkg_author** role to create, view, and modify Tanzu Kubernetes clusters within this organization, add the **Edit: Tanzu Kubernetes Guest Cluster** to that role. If you want the users with the **tkg_admin** role to create, view, modify, and delete Tanzu Kubernetes clusters within this organization, add the **Full Control: Tanzu Kubernetes Guest Cluster** right to the role.

3. Grant the specific user an Access Control List (ACL) by making the following REST API call.

   ```
   POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
   [version]:[UUID]/accessControls
    {
      "grantType" : "MembershipAccessControlGrant",
      "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
      "memberId" : "urn:vcloud:user:[User_ID]"
    }
   ```

   Access_level must be `ReadOnly`, `ReadWrite`, or `FullControl`. *User_ID* must be the ID of the user to which you want to grant the access to the defined entity.

   Users with the **tkg_viewer** role, described in the example, cannot grant ACL access. Users with the **tkg_author** or **tkg_admin** role can share access to a VMWARE:TKGCLUSTER entity with users who have the **tkg_viewer**, **tkg_author**, or **tkg_admin** role by granting them ACL access using the API request.

   You can also use REST API calls to revoke access or to view who has access to the entity. See the VMware Cloud Director REST API documentation.

Sharing Administrator Rights to Defined Entities

1. If you want to grant access to defined entities to tenants, publish the rights bundle of the defined entity type to a tenant organization. For example, for the creation and management of Tanzu Kubernetes clusters, you must publish the **vmware:tkgcluster Entitlement** rights bundle. See Publish or Unpublish a Rights Bundle to VMware Cloud Director.

   If you want to share the defined entity with a **system administrator**, skip this step.

2. Assign the **Administrator View: TYPE** or **Administrator Full Control: TYPE** right from the bundle to the user roles you want to have the specific level of access to the defined entity.

   For example, if you want the users with this role to view all Tanzu Kubernetes clusters within the organization, you must add the **Administrator View: Tanzu Kubernetes Guest Cluster** right to the role. If you want the users with this role to create, view, modify, and delete Tanzu Kubernetes clusters in all organizations, add the **Administrator Full Control: Tanzu Kubernetes Guest Cluster** right to the user role.

Users with the **Administrator Full Control: Tanzu Kubernetes Guest Cluster** right can grant ACL access to any VMWARE:TKGCLUSTER entity.

Changing the Owner of a Defined Entity

The owner of a defined entity or a user with the **Administrator Full Control: TYPE** right can transfer the ownership to another user by updating the defined entity model and changing the owner field with the ID of the new owner.

VMware Cloud Director Webhook Behaviors

To connect two different applications, you can use webhooks. By using webhooks, you can set up event notifications.

A webhook is an HTTP callback. When an event happens, a web application implementing webhooks broadcasts data about that event and sends it to a webhook URL from the application that you want to receive the information. For more information, see the Cloud Developer Platform.

In the context of VMware Cloud Director, you can configure webhooks by using webhook behaviors. Webhook behaviors send out a POST request to a remote webhook server. The body of the request contains information about the behavior invocation and the entity the behavior was invoked on. You can also customize the body by using a template. The webhook server response determines the result of the behavior invocation task. There are three different types of responses that the server can return.

The remote webhook server can be any server that VMware Cloud Director can reach. However, before creating a webhook behavior, you must verify that the endpoint of the webhook is secure.

- Verify that the webhook endpoint is an HTTPS endpoint.
- Verify that the organization of the user invoking the behavior trusts the webhook server certificate. This means that even if the certificate is present in a VMware Cloud Director trust store, if the organization of the user, who invokes the behavior does not trust the certificate, the webhook behavior will not run.
- You can add a certificate to the trust store by using the UI or the VMware Cloud Director API. See Managing Certificates Using Your VMware Cloud Director.

Creating Webhook Behaviors

Request:

```
"POST https"://host/cloudapi/1.0.0/interfaces/<interface_id>/behaviors{
   "name":"webhookBehavior",
   "execution":{
      "type":"WebHook",
      "id":"testWebHook",
      "href":"https://hooks.slack.com:443/services/T07UZFN0N/B01EW5NC42D/
rfjhHCGIwzuzQFrpPZiuLkIX",
      "key":"secretKey",
      "execution_properties":{
         "template":{
            "content":"<template_content_string>"
         },
         "_secure_token":"secureToken",
         "invocation_timeout":7
      }
   }
}
```

Field	Desciption
`type`	Required field. Must be `WebHook`.
`id`	Optional string field.
`href`	Required field for the URL that must receive requests from VMware Cloud Director.
`_internal_key`	Required field for the shared secret used for signing the requests sent to the webhook endpoint.
`invocation_timeout`	Optional field specifying the timeout in seconds for the response from the webhook server
`template.content`	Optional field for customization of the payload sent to the webhook server. You can provide a template as a string. You can add other fields to `execution_properties`, accessible to the template.
`_secure_`	Fields with prefix `_secure_` are optional. The fields are write-only and cannot be obtained through a GET request on the behavior. The field value gets encrypted before it is saved to the VMware Cloud Director database. The fields are accessible to the template.

Payload From VMware Cloud Director to the Webhook Server

There is a default format of the payload sent to the webhook server. You can also customize the payload by using a template.

Default payload example:

```
{
   "entityId":"urn:vcloud:entity:vmware:test_entity_type:b95d96ec-c294-4a64-
b5c4-9009abe6ab06",
   "typeId":"urn:vcloud:type:vmware:test_entity_type:1.0.0",
   "arguments":{
      "x":7
   },
   "_metadata":{
      "executionId":"testWebHook",
      "execution":{
         "href":"https://webhook.site/3ca4588f-c9f1-4c0f-911f-734ab598b2dc"
      },
      "invocation":{
      },
      "apiVersion":"36.0",
      "behaviorId":"urn:vcloud:behavior-
interface:webhookBehavior:vmware:test_interface_3:1.0.0",
      "requestId":"8312df21-712c-4b85-86d4-c9b00669662f",
      "executionType":"WebHook",
      "invocationId":"115c5b99-09e8-44f7-8189-4b9d96e067b1",
      "taskId":"a9e0556b-7699-4ded-b56b-c51fee659008"
   },
   "entity":{
      "cluster":{
         "name":"testCluster0"
      },
      "clusterState":{
         "host":"testHost",
         "status":"valid"
      }
   }
}
```

For custom payloads with a template, you can specify a template for the payload sent to the webhook server. If you do not specify a template, VMware Cloud Director sends the default request payload to the webhook server. The Apache FreeMarker template engine renders the payload from the provided template and the data model.

The data model represents all the data prepared for the template, in other words, all the data that you can include in the payload. The data model contains the invocation arguments of the webhook behavior, for example, arguments, metadata, execution properties, and entity information. The following example shows the tree-like structure of the data model.

```
+ - entityId
|
+ - typeId
|
+ - arguments
|
+ - arguments_string
|
+ - _execution_properties
|
+ - _metadata
|    |
|    + - executionId
|    + - behaviorId
|    + - executionType
|    + - taskId
|    + - execution
|    |    |
|    |    + - href
|    + - invocation
|    + - invocationId
|    + - requestId
|    + - apiVersion
```

```
|
+ - entity
|
+ - entity_string
```

Table 14-4. Invocation arguments

Argument	Description
`entityId`	ID of the invoked defined entity.
`typeId`	ID of the entity type of the invoked defined entity.
`arguments`	The arguments passed in the behavior invocation.
`arguments_string`	A JSON format string of arguments. You can use it if you want to add all the arguments to the payload.
`_execution_properties`	You can select all the values from the `execution_properties` invocation argument by key name.
`execution`	You can select all the values from the `execution` invocation argument by key name.
`invocation`	You can select all the values from the `invocation` argument by key name.
`entity`	A map of the entity content. You can select all values in the entity by key name.
`entity_string`	A JSON format string of entity.

For more information on the Apache FreeMarker expression language for the template for the payload, see https://freemarker.apache.org/docs/dgui_quickstart_template.html.

Sample template:

```
<#assign header_Content\-Type= "application/json" />
{
"text": "Behavior with id ${_metadata.behaviorId} was executed on entity with id $
{entityId}"
}
```

You can specify custom headers that you want to add to the POST request sent to the webhook servers. You can use the webhook template for adding custom headers which are variables in the template with the prefix `header_`. For example, you can specify the value for the `Authorization` header by adding the following line to the template:

```
<#assign header_Authorization = "${_execution_properties._secure_token}" />
```

Payload From the Webhook Server to VMware Cloud Director

- Default response

  The default payload from the webhook server to VMware Cloud Director must contain the following.

  - The response can either have no `Content-Type` header or a `Content-Type` header with `text/plain` value.
  - The response body must be a string.
  - The body of the response is used as the result of the behavior invocation. The status for the behavior invocation task is `success`. The task result is set to the body of the response.

- Single task update response

  Apart from the behavior result, the task update response can set some other behavior invocation task properties like `status`, `details`, `operation`, `error`, `progress`, and `result`. Because this is a one-time task update, the response must complete the task. If the response does not set the task status to `success`, `error`, or `aborted`, then the task fails with an error. The error message indicates that the status was not acceptable.

  - The response must have a `Content-Type` header with `application/vnd.vmware.vcloud.task+json` value.
  - The response body must contain a JSON representation of the `TaskType` class containing the task properties you want to modify.
  - Sample response body with status `success`:

    ```
    {
       "status":"success",
       "details":"example details",
       "operation":"example operation",
       "progress":100,
       "result":{
          "resultContent":"example result"
       }
    }
    ```

  - Sample response body with status `error`:

    ```
    {
       "status":"error",
       "details":"example details",
       "operation":"example operation",
       "progress":50,
       "error":{
          "majorErrorCode":404,
          "minorErrorCode":"ERROR",
          "message":"example error message"
       }
    }
    ```

- Continuous task update response

The webhook server can send multiple task updates by using a multi-part HTTP response. Each update is a separate body part of the response body. The last body part of the webhook server response body must finish the task. If the response body does not finish the task, the task fails with an error.

- The response must have a `Content-Type` header with `multipart/form-data; boundary=...` value.
- The response body must start and end with a boundary string `--<boundary_string>`. Each part of the response body must end in a boundary string. You must specify the boundary in the `Content-Type` header of the HTTP response from the webhook server.

```
Headers:
...
Content-Type: multipart/form-data; boundary=<boundary_string>

Body:
--<boundary_string>
Content-Type: application/vnd.vmware.vcloud.task+json
{
"details": "example details",
"operation": "example operation",
"progress": 50
}
--<boundary_string>
Content-Type: application/vnd.vmware.vcloud.task+json
{
"status": "success",
"progress": 100,
"result": {
"resultContent": "example result"
}
}
--<boundary_string>
```

The body parts in the response body must be in the format for a task update or the format for a final update.

Task update example:

```
Content-Type: application/vnd.vmware.vcloud.task+json
{
"details": "example details",
"operation": "example operation",
"progress": 50
}
```

Final update example:

```
Content-Type: text/plain
<string>
```

Authentication of the Webhook Behavior Requests

Hash-based message authentication code (HMAC) authentication secures webhook behavior requests. HMAC is a mechanism ensuring the authenticity and integrity of HTTP requests. To ensure the authenticity and integrity, HMAC includes two custom headers to each HTTP request. The custom headers are a signature header and a digest. For VMware Cloud Director, the signature header is `x-vcloud-signature` and the digest is `x-vcloud-digest`.

The signature header `x-vcloud-signature` is a custom header sent with each webhook request. The signature header consists of an HMACSHA512 algorithm, headers, and a VMware Cloud Director generated signature. The headers show what is in the base string which is signed to create the signature.

Table 14-5. Header Fields

Field	Description
`host`	The webhook server host
`date`	Date of the request
`(request-target)`	Linked lowercase HTTP method, ASCII space, and request path headers. For example, `post /webhook`.
`digest`	SHA-512 digest of the request body

To generate the signature header, you need a shared secret. The shared secret is a string that only VMware Cloud Director and the webhook server know.

The digest header `x-vcloud-digest` is a Base64-encoded SHA-512 digest of the request body.

Each webhook request from VMware Cloud Director can be verified by generating the signature using the shared secret and comparing it to the signature in the signature header from VMware Cloud Director.

Invoking Webhook Behaviors

You can invoke webhook behaviors like any other behavior.

```
{
"arguments": {
"argument1": "data1",
"argument2": "data2",
...
 }
}
```

Managing Custom Entities in VMware Cloud Director

The custom entity definitions in VMware Cloud Director are object types that are bound to VMware Aria Automation Orchestrator object types.

When a service provider publishes a custom entity definitions to either another service provider, or to one or more tenants, users VMware Cloud Director can own, manage, and change these types according to their needs. By executing services, service provider users and organization users can instantiate the custom entities and apply actions over the instances of the objects.

Search for a Custom Entity in Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can search for a custom entity by its name.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 in Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can modify the name and the description of a custom entity. You cannot change the type of the entity or the VMware Aria Automation 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.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 in Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can create a custom entity and map it to an existing VMware Aria Automation Orchestrator object type.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation Orchestrator type to which the entity is mapped, the type of the entity, and a description, if available.

2 To add a new custom entity, click **New**.

   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 VMware Aria Automation Orchestrator that you will use to map the custom entity definition. **Note** If you have more than one VMware Aria Automation 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 VMware Aria Automation 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.

Results

The new custom entity definition appears in the card view.

Custom Entity Instances in VMware Cloud Director

Running a VMware Aria Automation Orchestrator workflow with an input parameter being an object type that is already defined as a custom entity definition in VMware Cloud Director shows the output parameter as an instance of a custom entity.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 **Intances**.

   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 In VMware Cloud Director

By associating an action to a custom entity definition, you can execute a set of VMware Aria Automation Orchestrator workflows on the instances of a particular custom entity.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 VMware Aria Automation 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 in VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can remove a VMware Aria Automation Orchestrator workflow from the list of associated actions.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 window opens.

3 Select the workflow you want to remove and click **Dissociate Action**.

   The VMware Aria Automation Orchestrator workflow is no longer associated with the custom entity.

Publish a Custom Entity to VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can publish a custom entity so users from other tenants or service providers can run workflows using the custom entity instances as input parameters.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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 window 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 From VMware Cloud Director

Using the VMware Cloud Director Service Provider Admin Portal, 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 VMware Aria Automation Orchestrator type to a different custom entity.

Procedure

1 From the top navigation bar, select **Libraries**.

   a From the left panel, 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 VMware Aria Automation 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.

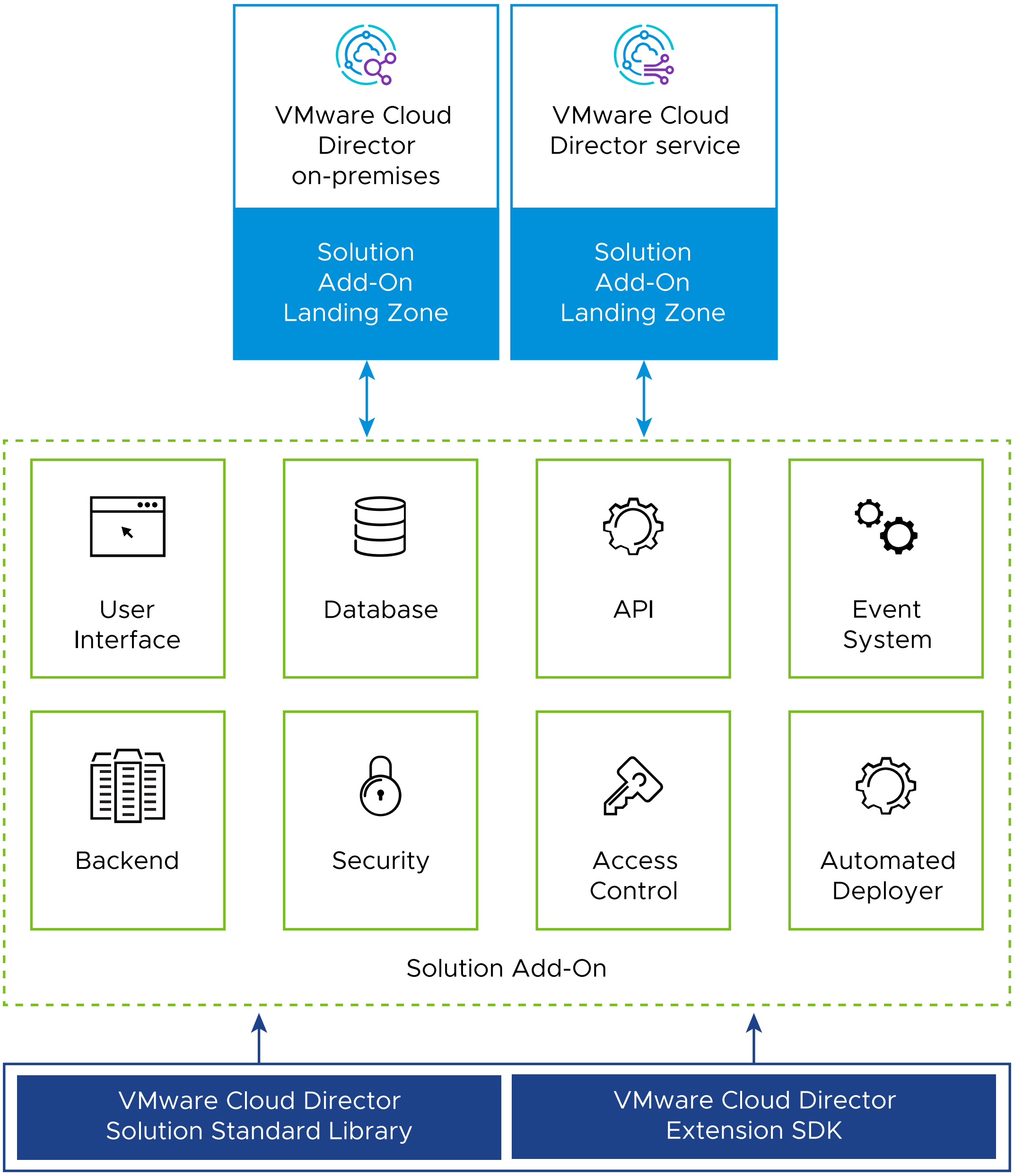
Using Solution Add-Ons with VMware Cloud Director

15

You can use VMware Cloud Director Solution Add-Ons UI to extend your VMware Cloud Director offering with value-added functionalities. Through the UI, you can manage the resources and life cycle of solutions that are custom-built to extend the functionality of VMware Cloud Director.

A solution add-on is the representation of a solution that is custom built for VMware Cloud Director in the VMware Cloud Director extensibility ecosystem. A solution add-on can encapsulate UI and API VMware Cloud Director extensions together with their backend services and lifecycle management. Solution add-ons are distributed as `.iso` files with an embedded installer for 64 bit Linux, Windows, and MacOS operating systems. A solution add-on can contain numerous elements: UI plugins, vApps, users, roles, runtime defined entities, and more.

The VMware Cloud Director Solution Standard Library and the VMware Cloud Director Extension SDK are leveraged by vendors for the creation of solution add-ons. You can install a solution add-on by running the deployer that is embedded in the `.iso` file, or by uploading the file in the Solution Add-On Landing Zone and using the Solution Add-On management UI.


VMware Cloud Director on-premises
Solution Add-On Landing Zone
VMware Cloud Director service
Solution Add-On Landing Zone
User Interface
Database
API
Event System
Backend
Security
Access Control
Automated Deployer
Solution Add-On
VMware Cloud Director Solution Standard Library
VMware Cloud Director Extension SDK

The Solution Add-On Landing Zone is a part of the provider management plane that represents a pool of compute, storage and networking resources dedicated to hosting, managing, and running solution add-ons on behalf of the cloud provider. You can manage the Solution Add-On Landing Zone by using the Solution Add-On Management UI plugin or through the Defined Entity API.

In the Solution Add-On Landing Zone, you can select the resources to use for the upload of solution add-on `.iso` files and, if necessary, for the deployment of the backend services that are contained in the `.iso` files. You configure your Solution Add-On Landing Zone by selecting a VMware Cloud Director organization to provide the resources for the Solution Add-On Landing Zone, a catalog, and, if necessary for your solution add-on's backend services, one or more organization VDCs. For each organization VDC that you select, you must specify the networks, storage policies, and, optionally, the compute policies that you want to attach to the solution add-ons. Additionally, each solution add-on can have a set of specific VMware Cloud Director configuration requirements that are defined as capabilities.

Starting with VMware Cloud Director 10.5, when a new version of a solution add-on becomes available, you can upgrade your existing solution add-on instances to the new version. You can publish solution add-ons to some or to all tenants in your environment.

To create solution add-ons, you can use the VMware Cloud Director Extension SDK.

Key Roles in the VMware Cloud Director Extension SDK Ecosystem

Vendor

Vendors are the creators of solution add-ons who use the VMware Cloud Director Extension SDK to create services that complement VMware Cloud Director, such as Container Service Extension, third-party software vendors, Kubernetes service, and others.

Provider

Providers are the operators of solution add-ons in the VMware Cloud Director on-premises or VMware Cloud Director service environment.

Tenant

Tenants are the consumers of the business outcomes brought about by a solution add-on, for example, self-service provisioning of Kubernetes clusters, Kubernetes operators, databases, UI extensions with back-office properties, and more.

Read the following topics next:

- Configure Your Solution Add-On Landing Zone in VMware Cloud Director
- Edit the Settings of Your Solution Add-On Landing Zone in VMware Cloud Director
- Upload a Solution Add-On to Your VMware Cloud Director
- Deploy an Instance of a Solution Add-On to Your VMware Cloud Director
- Upgrade a Solution Add-On Instance in VMware Cloud Director
- Publish a Solution Add-On Instance To a VMware Cloud Director Organization
- Unpublish a Solution Add-On Instance To a VMware Cloud Director Organization
- Delete an Instance of a Solution Add-On From VMware Cloud Director
- Remove a Solution Add-On From VMware Cloud Director
- View the Task Details for a Solution Add-On Instance in VMware Cloud Director
- Reupload a Missing ISO File to VMware Cloud Director

Configure Your Solution Add-On Landing Zone in VMware Cloud Director

The Solution Add-On Landing Zone is a runtime defined entity that encapsulates the location of specific resources that are required for the unattended installation or upgrade of any solution add-on in VMware Cloud Director.

You configure your Solution Add-On Landing Zone by selecting a VMware Cloud Director organization to provide the resources for the Solution Add-On Landing Zone, a catalog where the solution add-ons are uploaded, and, if necessary, one or more organization VDCs.

If you don't use an organization VDC for your Solution Add-On Landing Zone, you will not be able to instantiate Solution Add-Ons that require backend services.

For each organization VDC that you select, you must specify the networks, compute policies and storage policies you want to attach to the solution add-ons. Additionally, each solution add-on can have a set of specific VMware Cloud Director configuration requirements that are defined as capabilities.

Prerequisites

- Verify that you have enough compute and memory resources in each organization VDC or organization that you plan to use for the Solution Add-On Landing Zone.
- Verify that the runtime lease for the vApps in each organization or organization VDC that you use for the Solution Add-On Landing Zone is set to **Unlimited**. For details, see Understanding Leases in VMware Cloud Director.
- Create a catalog to store the `.iso` files of your solution add-ons in the organization that you plan to use for the Solution Add-On Landing Zone. When creating the catalog, if you are going to use an organization VDC for the Solution Add-On Landing Zone, toggle on the **Pre-provision on specific storage policy** option and from the drop-down menu, select the organization VDC that you will use. For details, see *Create a Catalog* in the *VMware Cloud Director Tenant Guide*.
- Verify that each organization VDC network that you use for the Solution Add-On Landing Zone has access to the public service provider endpoints of the VMware Cloud Director API.
- Verify that you either configured static IP pools or enabled DHCP for each organization VDC network that you use for the Solution Add-On Landing Zone.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. Click **Configure**.
3. In the **What is a Solution Add-On Landing Zone** page, familiarize yourself with the provided information, and click **Next**.

4. In the **General Settings** page, select an organization to provide resources for the Solution Add-On Landing Zone.

   Important Once you make this selection, you cannot change it.

5. From the drop-down menu, select a catalog to store the `.iso` files for your solution add-ons.
6. If you plan to deploy solution add-ons that use backend services, select at least one organization VDC and click **Next**.
7. If you selected an organization VDC in which to deploy the backend services for your solution add-ons, click the vertical ellipsis (⋮) and click **Configure**.
8. If you selected an organization VDC in which to deploy the backend services for your solution add-ons, select an organization VDC network to connect to your solution add-ons for each of the VDCs that participate in the landing zone.
9. If you added an organization VDC to the landing zone, and you want to add more organization VDC networks, click **Add Network** and select a network from the list.
10. If you added an organization VDC to the landing zone, click the **Compute Policies** tab and select a compute policy for the solution add-ons.
11. If you added an organization VDC to the landing zone, click the **Storage Policies** tab and select at least one storage policy for the solution add-ons.
12. Click **Save** and then click **Next**.
13. Review your settings and click **Finish**.

Edit the Settings of Your Solution Add-On Landing Zone in VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can edit some of the settings of your Solution Add-On Landing Zone after its initial configuration.

Changing some of the settings of your Solution Add-On Landing Zone might require additional steps. For example, selecting another catalog to use in the Solution Add-On Landing Zone does not affect the solution add-ons that you already installed, but prevents you from running day-2 operations on them. To ensure that you can run day-2 operations on the add-ons that are already installed after selecting a new catalog, you must Reupload a Missing ISO File to VMware Cloud Director.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. Click **Configure Landing Zone**.

3. Change the catalog where you store the `.iso` files for you solution add-ons.

   a. Click **Edit**.

   b. From the drop-down menu, select a new catalog and click **Save**.

4. Include an organization VDC in the Solution Add-On Landing Zone.

   a. Click **Include VDC**.

   b. From the drop-down menu, select an organization VDC to include in the landing zone.

   c. Click the **Network** tab and select at least one organization VDC network for your solution add-ons.

   d. To add a new network, click **Add Network** and select an organization VDC network from the list.

   e. Click the **Compute Policies** tab and select a compute policy for the solution add-ons.

   f. Click the **Storage Policies** tab and select at least one storage policy.

   g. Click **Include**.

5. Modify the settings of a participating organization VDC.

   a. On the left of the organization VDC name, click the vertical ellipsis ⋮ , and click **Configure**.

   b. To add a new organization VDC network, click **Add Network** and select an organization VDC network from the list.

   c. Click the **Compute Policies** tab and select a new compute policy for the solution add-ons.

   d. Click the **Storage Policies** tab and select at least one storage policy for the solution add-ons.

   e. Click **Save**.

6. Change the default VDC of the Solution Add-On Landing Zone.

   If you have more than one organization VDC participating in your Solution Add-On Landing Zone, you can change the default VDC. After the change, all new solution add-ons deploy in the new default VDC unless a solution add-on needs specific capabilities which are satisfied by another VDC.

   a. On the left of the name of the organization VDC that you want to set as default, click the vertical ellipsis ⋮ , and click **Make Default**.

7. To exclude an organization VDC from the Solution Add-On Landing Zone, click the vertical ellipsis ⋮ , and click **Exclude**.

Upload a Solution Add-On to Your VMware Cloud Director

To deploy an instance of a solution add-on, in the VMware Cloud Director Service Provider Admin Portal, first you must upload its `.iso` file to the Solution Add-On Landing Zone.

You can upload more than one version of a solution add-on.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. Click **Upload**.
3. Browse to the solution add-on `.iso` file.
4. If you want to create an instance of the solution add-on after the upload is completed, select the check box.
5. Click **Upload**.
6. If prompted, verify that you trust the certificates of the solution add-on.
7. Click **Finish**.

What to do next

If you chose to create an instance of the solution add-on, follow the prompts and enter the required information to deploy the instance.

Deploy an Instance of a Solution Add-On to Your VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can deploy an instance of a solution add-on with customized input parameters.

Prerequisites

Verify that you uploaded the solution add-on that you want to deploy.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. In the card of the solution add-on, click **New Instance**.
3. On the **Accept Licenses** page, read the license agreements associated with the solution add-on and click **I Agree**.
4. Enter the input parameters for the solution add-on instance.
5. Review your settings and click **Finish**.

Upgrade a Solution Add-On Instance in VMware Cloud Director

When a new version of a solution add-on in your environment becomes available, you can upgrade your existing solution add-on instances.

Prerequisites

- Verify that upgrade is supported for the current version of your solution add-on instance.
- Upload the `.iso` file for the new solution add-on version to the Solution Add-On Landing Zone.
- Verify that the solution add-on instance that you want to upgrade is running.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. In the card of the solution add-on, click **Instances**.
3. On the left of the name of the solution add-on instance that you want to upgrade, click the vertical ellipsis (⋮) and select **Upgrade**.
4. Select the version to which to upgrade.
5. If there are any changes to the license agreements associated with the solution add-on, read them and click **I Agree**.
6. If there are any changes to the input parameters for the solution add-on instance, enter the new values, and click **Next**.
7. Review your settings and click **Finish**.

What to do next

If the upgrade fails, you can roll back to the previous state of the solution add-on instance or retry the upgrade.

Roll Back a Failed Upgrade of a Solution Add-On Instance in VMware Cloud Director

If the upgrade of a solution add-on instance fails, in the VMware Cloud Director Service Provider Admin Portal, you can either retry the upgrade or roll it back.

Procedure

1. In the top navigation bar, click **More > Solution Add-On Management**.
2. In the card of the solution add-on, click **Instances**.

3 On the left of the name of the solution add-on instance, click the vertical ellipsis (⋮) and select **Rollback**.

   If the operation is successful, the instance is rolled back to its previous version.

4 (Optional) To attempt the upgrade again, click the vertical ellipsis (⋮) and select **Retry Upgrade**.

Publish a Solution Add-On Instance To a VMware Cloud Director Organization

As a VMware Cloud Director **service provider**, you can publish solution add-on instances to some or to all your tenants.

Vendors can decide whether to include tenant access to some of the elements in a solution add-on, such as global roles, rights bundles, defined entity types and UI plug-ins. If a **vendor** configured a solution add-on element to be shared with tenants, when a **service provider** publishes the solution add-on instance to a tenant, these elements are also shared with the tenant. For more details on configuring solution add-on elements and scope, see VMware Cloud Director Extension Developer Guide.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 On the card of the solution add-on, click **Details**.

3 Select the **Instances** tab.

4 On the left of the name of the solution add-on instance, click the vertical ellipsis (⋮), and select **Publish**.

5 Select the organizations to which you want to publish the solution add-on, and click **Save**.

   For VMware Cloud Director 10.5.0, to publish the solution add-on to all organizations in your environment, toggle on the **Publish to All Tenants** option.

   Important If the **Publish to All Tenants** option is activated, VMware Cloud Director also publishes the solution add-on instance to all organizations that you create in the future.

Results

The solution add-on instance becomes visible to the organizations to which you published it.

What to do next

If necessary, you can unpublish the solution add-on to some or to all of the organizations to which you published it.

Unpublish a Solution Add-On Instance To a VMware Cloud Director Organization

If you want to restrict tenant access to a solution add-on instance that you published, in the VMware Cloud Director Service Provider Admin Portal, you can unpublish it.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 In the card of the solution add-on, click **Instances**.

3 On the left of the name of the solution add-on instance that you want to unpublish, click the vertical ellipsis (⋮) and select **Unpublish**.

4 Choose one of the options.

- To unpublish the solution add-on to all the organizations in your environment, toggle on the **Unpublish to All Tenants** option.
- To unpublish the solution add-on instance to one or more organizations in your environment, select their names from the list.

5 Click **Save**.

Results

The solution add-on instance becomes inaccessible to the organizations to which you unpublished it.

Delete an Instance of a Solution Add-On From VMware Cloud Director

If you no longer need a specific instance of solution add-on, you can remove it by using the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 In the card of the solution add-on, click **Details**.

3 On the left of the name of the solution add-on instance that you want to delete, click the vertical ellipsis (⋮) and select **Remove**.

Remove a Solution Add-On From VMware Cloud Director

If you no longer need a solution add-on in your landing zone, you can delete it from VMware Cloud Director.

You can delete a solution add-on from your landing zone.

Prerequisites

Verify that you removed all the instances of the solution add-on.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 In the card of the solution add-on, click the vertical ellipsis ⋮ and select **Remove**.

View the Task Details for a Solution Add-On Instance in VMware Cloud Director

In the VMware Cloud Director Service Provider Admin Portal, you can troubleshoot task failures in your solution add-on management UI.

You can check the details for the tasks and subtasks that you run for each solution add-on instance in your environment.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 Select a solution add-on.

3 Click the **Instances** tab.

4 Click the expansion arrows for the instance for which you want to see the task details.

5 On the right, click the **Tasks** tab.

   A list of tasks that you ran on this solution add-on instance appears, together with their status.

6 Click the expansion arrows for the task for which you want to view details.

   A list of subtasks and their status appears.

Reupload a Missing ISO File to VMware Cloud Director

If solution add-on ISO file is missing from the catalog specified in your Solution Add-On Landing Zone, this prevents you from running day-2 operations on the solution add-on instances. To secure proper functioning of the add-ons instances that are already deployed, reupload the missing ISO files by using the VMware Cloud Director Service Provider Admin Portal.

Procedure

1 In the top navigation bar, click **More > Solution Add-On Management**.

2 Browse to the solution add-on `.iso` file and click **Upload**.

VMware Cloud Director Cell Management Tool Reference

16

The cell management tool is a command-line utility that you can use to manage a VMware Cloud Director cell or database. You must use superuser or system administrator credentials for most operations.

The cell management tool is installed in `/opt/vmware/vcloud-director/bin/`. You can use it to run a single command or run it as an interactive shell.

Some functions of the cell management tool are more useful during the VMware Cloud Director deployment and initial configuration, while others are more useful for the subsequent administration of VMware Cloud Director. For this reason, you can find some of the cell management tool documentation in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*. See VMware Cloud Director Cell Management Tool Reference.

Listing Available Commands

To list the available cell management tool commands, use the following command line.

```
./cell-management-tool -h
```

Using Shell Mode

You can run the cell management tool as an interactive shell by invoking it with no arguments, as shown here.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350
Type "help" for available subcommands.
cmt>
```

While in shell mode, you can type any cell management tool command at the `cmt>` prompt, as shown in this example.

```
cmt>cell -h
usage: cell [options]
               -a,--application-states     display the state of each application
                                           on the cell [DEPRECATED - use the
                                           cell-application command instead]
               -h,--help                   print this message
               -i,--pid <arg>              the process id of the cell [REQUIRED
                                           if username is not specified]
               -m,--maintenance <arg>      gracefully enter maintenance mode on
                                           the cell
               -p,--password <arg>         administrator password [OPTIONAL]
               -q,--quiesce <arg>          quiesce activity on the cell
               -s,--shutdown               gracefully shutdown the cell
               -t,--status                 display activity on the cell
               -tt,--status-verbose        display a verbose description of
                                           activity on the cell
               -u,--username <arg>         administrator username [REQUIRED if
                                           pid is not specified]
Note: You will be prompted for administrator password if not entered in command
line.
cmt>
```

The command returns to the `cmt>` prompt when it finishes running. To exit the shell mode, type **`exit`** at the `cmt>` prompt.

Example: Cell Management Tool Usage Help

This example runs a single, non-interactive command that lists available shell management tool commands.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h

usage: cell-management-tool
-h,--help   print this message

Available commands:
cell - Manipulates the Cell and core components
certificates - Reconfigures the SSL certificates for the cell
.
.
.

For command specific help:
 cell-management-tool <commandName> -h
```

Starting with VMware Cloud Director 10.3, to troubleshoot failed access to the VMware Cloud Director UI, you must use the `https://{api_host}/cloudapi/1.0.0/site/settings/cors` API endpoint instead of a CMT command. For more information, see Troubleshoot Failed Access to the VMware Cloud Director User Interface.

- Deactivate the Service Provider Access to the Legacy VMware Cloud Director API Endpoint

  Starting with VMware Cloud Director 10.0, you can use separate VMware Cloud Director OpenAPI login endpoints for the service provider and tenant access to VMware Cloud Director.

- Detecting and Repairing Corrupted Scheduler Data in VMware Cloud Director

  VMware Cloud Director uses the Quartz job scheduler to co-ordinate asynchronous operations (jobs) running on the system. If the Quartz scheduler database becomes corrupted, you might not be able to quiesce the system successfully. Use the `fix-scheduler-data` command of the cell management tool to scan the database for corrupt scheduler data and repair that data as needed.

- Clear the Console Proxy Settings in VMware Cloud Director

  Starting with VMware Cloud Director 10.4, both the console proxy traffic and HTTPS communications go over the default 443 port. To clear all network settings related to the legacy proxy console implementation, you can use the `clear-console-proxy-settings` command of the cell management tool.

- Importing SSL Certificates from External Services to VMware Cloud Director

  Use the `import-trusted-certificates` command of the cell management tool to import certificates for use in establishing secure connections to external services like AMQP and the VMware Cloud Director database.

- Import Endpoints Certificates from vSphere Resources to VMware Cloud Director

  After upgrade, use the `trust-infra-certs` command of the cell management tool to collect and import certificates from the vSphere resources in your environment to the VMware Cloud Director database.

- Detect and Fix Resource Pool Mismatches between VMware Cloud Director and vCenter Server

  You can detect and fix resource pool mismatches between VMware Cloud Director and vCenter Server by using the cell management tool.

- Configure a Test Connection Denylist in VMware Cloud Director

  After installation or upgrade, use the `manage-test-connection-denylist` command of the cell management tool to block access to internal hosts before providing tenants with access to the VMware Cloud Director network.

- Configure Metrics Collection and Publishing in VMware Cloud Director

  You can use the `configure-metrics` command of the VMware Cloud Director cell management tool to configure the set of metrics to collect.

- Configuring a Cassandra Metrics Database in VMware Cloud Director

  Use the `cassandra` command of the cell management tool to connect the cell to an optional metrics database.

- Recovering the VMware Cloud Director System Administrator Password

  If you know the VMware Cloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the VMware Cloud Director system administrator password.

- Update the Failure Status of a Task in VMware Cloud Director

  Use the `fail-tasks` command of the VMware Cloud Director cell management tool to update the completion status associated with tasks that were running when the cell was deliberately shut down. You cannot use the `fail-tasks` command unless all cells have been shut down.

- Configure Audit Message Handling in VMware Cloud Director

  Use the `configure-audit-syslog` command of the VMware Cloud Director cell management tool to configure the way the system logs audit messages.

- Configuring Email Templates in VMware Cloud Director

  To manage the templates that the system uses when creating email alerts, you can use the `manage-email` command of the VMware Cloud Director cell management tool.

- Finding Orphaned VMs in VMware Cloud Director

  Use the `find-orphan-vms` command of the cell management tool to find references to virtual machines that are present in the vCenter database but not in the VMware Cloud Director database.

- Join or Leave the VMware Customer Experience Improvement Program

  To join or leave the VMware Customer Experience Improvement Program (CEIP), you can use the `configure-ceip` subcommand of the VMware Cloud Director cell management tool.

- Updating Application Configuration Settings in VMware Cloud Director

  With the `manage-config` subcommand of the VMware Cloud Director cell management tool, you can update different application configuration settings such as catalog throttling activities.

- Configuring Catalog Synchronization Throttling in VMware Cloud Director

  When you have many catalog items published to or subscribed from other organizations, to avoid overloading the system during catalog synchronizations, you can configure catalog synchronization throttling.

- Debugging vCenter VM Discovery in VMware Cloud Director

  By using the `debug-auto-import` subcommand of the cell management tool, you can investigate the reason for which the mechanism for discovering vApps skips one or more vCenter VMs.

- Regenerating MAC Addresses for Multisite Stretched Networks in VMware Cloud Director

  If you associate two VMware Cloud Director sites that are configured with the same installation ID, you might encounter MAC address conflicts in stretched networks across these sites. To avoid such conflicts, you must regenerate the MAC addresses in one of the sites based on a custom seed that is different from the installation ID.

- Activate a Lazy Resource Apportioning for an Elastic Flex Organization VDC in VMware Cloud Director

  Starting with VMware Cloud Director 10.5.1.1, for an elastic Flex organization VDC, you can activate a setting for reconfiguration of the resource pools backing the VDC only when necessary.

Deactivate the Service Provider Access to the Legacy VMware Cloud Director API Endpoint

Starting with VMware Cloud Director 10.0, you can use separate VMware Cloud Director OpenAPI login endpoints for the service provider and tenant access to VMware Cloud Director.

You can use two new OpenAPI endpoints to increase the security by restricting the access to VMware Cloud Director.

- `/cloudapi/1.0.0/sessions/provider` - OpenAPI endpoint for the service provider login. Tenants cannot access VMware Cloud Director by using this endpoint.
- `/cloudapi/1.0.0/sessions/` - OpenAPI endpoint for the tenant login. Service providers cannot access VMware Cloud Director by using this endpoint.

By default, provider administrators and organization users can access VMware Cloud Director by logging into the `/api/sessions` API endpoint.

By using the `manage-config` subcommand of the cell management tool, you can deactivate the service provider access to the `/api/sessions` API endpoint and, as a result, limit the provider login to the new `/cloudapi/1.0.0/sessions/provider` OpenAPI endpoint that is accessible only to service providers.

Note When you deactivate the service provider access to the `/api/sessions` API endpoint, service provider requests that supply only a SAML token in the authorization header will fail for all legacy API endpoints.

Procedure

1. Log in or SSH as **`root`** to the OS of any of the VMware Cloud Director cells.
2. To block the provider access to the `/api/sessions` API endpoint, use the cell management tool and run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v true
```

Results

The `/api/sessions` API endpoint is no longer accessible to service providers. Service providers can use the new OpenAPI endpoint `/cloudapi/1.0.0/sessions/provider` to access VMware Cloud Director. Tenants can access VMware Cloud Director by using both the `/api/sessions` API endpoint and the new `/cloudapi/1.0.0/sessions/` OpenAPI endpoint.

What to do next

To enable the provider access to the `/api/sessions` API endpoint, run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

Detecting and Repairing Corrupted Scheduler Data in VMware Cloud Director

VMware Cloud Director uses the Quartz job scheduler to co-ordinate asynchronous operations (jobs) running on the system. If the Quartz scheduler database becomes corrupted, you might not be able to quiesce the system successfully. Use the `fix-scheduler-data` command of the cell management tool to scan the database for corrupt scheduler data and repair that data as needed.

To scan database for corrupt scheduler data, use a command line with the following form:

```
cell-management-tool fix-scheduler-data options
```

Table 16-1. Cell Management Tool Options and Arguments, `fix-scheduler-data` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--dbuser`	The user name of the VMware Cloud Director database user.	Must be supplied on the command line.
`--dbpassword`	The password of the VMware Cloud Director database user.	Prompted for if not supplied.

Clear the Console Proxy Settings in VMware Cloud Director

Starting with VMware Cloud Director 10.4, both the console proxy traffic and HTTPS communications go over the default 443 port. To clear all network settings related to the legacy proxy console implementation, you can use the `clear-console-proxy-settings` command of the cell management tool.

The `clear-console-proxy-settings` command of the cell management tool clears the legacy console proxy IP address, port, and certificate settings.

Note VMware Cloud Director 10.4.1 and later do not support the legacy implementation of the console proxy feature.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director server cell as **root**.

2 To clear all settings related to the legacy console proxy implementation, run the following command.

```
/opt/vmware/vcloud-director/bin/cell-management-toolclear-console-proxy-settingsoption
```

Table 16-2. Cell Management Tool Options and Arguments, `clear-console-proxy-settings` Subcommand

Option	Argument	Description
`-c`, `--c`	Full pathname to the `global.properties` file	Defaults to `VCLOUD_HOME/etc/global.properties`.
`--help (-h)`	None	Provides a summary of available commands in this category.
`-r`, `--r`	Full pathname to the `responses.properties` file	Defaults to `VCLOUD_HOME/etc/responses.properties`.

Importing SSL Certificates from External Services to VMware Cloud Director

Use the `import-trusted-certificates` command of the cell management tool to import certificates for use in establishing secure connections to external services like AMQP and the VMware Cloud Director database.

Before it can make a secure connection to an external service, VMware Cloud Director must establish a valid chain of trust for that service by importing the service's certificates into its own truststore. To import trusted certificates to the cell's truststore, use a command with the following form:

```
cell-management-tool import-trusted-certificates options
```

Table 16-3. Cell Management Tool Options and Arguments, `import-trusted-certificates` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--force`	None	Overwrites the existing certificates in the destination truststore.
`--source`	path name	Full path name to source PEM file.

Example: Importing Trusted Certificates

This example imports the certificates from `/tmp/demo.pem` to the VMware Cloud Director local truststore at `/opt/vmware/vcloud-director/etc/truststore.pem`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-
certificates --source /tmp/demo.pem
```

Import Endpoints Certificates from vSphere Resources to VMware Cloud Director

After upgrade, use the `trust-infra-certs` command of the cell management tool to collect and import certificates from the vSphere resources in your environment to the VMware Cloud Director database.

The `trust-infra-certs` command of the cell management tool automatically gathers the SSL certificates from the vSphere resources in your environment and imports them to the VMware Cloud Director database.

Prerequisites

Verify that the vCenter Server and NSX-V Manager instances for which you want to import endpoints are up and running.

Procedure

1 Log in or SSH as root to the OS of the VMware Cloud Director cell.

2 Run the command in the following form.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

Table 16-4. Cell Management Tool Options and Arguments, `trust-infra-certs` Subcommand

Option	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--vsphere`	None	Prompts you to trust certificates for all registered vCenter Server, NSX Data Center for vSphere, and NSX instances in this installation.
`--unattended`	None	Optional. The command does not prompt for further input when invoked with this option. All infrastructure certificates are automatically trusted.

Example: Trust and Import All Certificates from vSphere Resources Endpoints

To trust and import the certificates from your vSphere resources endpoints without being prompted for further input, run the command with the following options.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

Detect and Fix Resource Pool Mismatches between VMware Cloud Director and vCenter Server

You can detect and fix resource pool mismatches between VMware Cloud Director and vCenter Server by using the cell management tool.

Starting with VMware Cloud Director 10.4.1, you can detect and fix mismatches between the resource pools in the inventory of VMware Cloud Director and the inventory of vCenter Server by using the cell management tool. The `detect-rp-mismatches` subcommand of the cell management tool detects a new resource pool that was added or recreated in the vCenter Server inventory and includes it as a backing resource of the provider VDCs and organization VDCs in VMware Cloud Director.

Prerequisites

Verify that VMware Cloud Director is up and running.

Procedure

1 Log in or SSH to the OS of the VMware Cloud Director cell as **root**.

2 Run the command in the following form.

```
/opt/vmware/vcloud-director/bin/cell-management-tool detect-rp-mismatches options
```

Table 16-5. Cell Management Tool Options and Arguments, `detect-rp-mismatches` Subcommand

Option	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--detect-mismatch-with-vc`	None	Detect a resource pool mismatch between the vCenter Serverinventory and the provider VDCs and organization VDCs in your VMware Cloud Director environment. If you use this option without further input, such as the optional `--vdcs` and `--pvdcs`, the command runs for all VDCs and PVDs.

Table 16-5. Cell Management Tool Options and Arguments, `detect-rp-mismatches` Subcommand (continued)

Option	Argument	Description
`--fix-mismatch-with-vc`	None	Fix the resource pool mismatch between the vCenter inventory and VMware Cloud Director for both the provider VDCs and the organization VDCs in your environment. If you use this option without further input, such as the optional `--vdcs` and `--pvdcs`, the command runs for all VDCs and PVDs. After you run the command, follow the cell management tool prompts and provide the necessary input to recreate the resource pool in the vCenter inventory, if necessary. To sync the updated vCenter resource pool inventory to the VMware Cloud Director database, make sure the VMware Cloud Directorinstance is running. **Note** If the resource pool was deleted or recreated in the vCenter Server instance, follow the command prompts to recreate it and to let the updated inventory sync with the running VMware Cloud Director instance. Provide the necessary information about the recreated resource pool. When the resource pool mismatch fix completes, a notification appears. If there were VMs that were originally under the resource pool which was recreated and these VMs were moved to another one upon the resource pool deletion, the cell management tool provides a list of all the VMs that you must move back under the recreated resource pool to complete the fix.

Table 16-5. Cell Management Tool Options and Arguments, `detect-rp-mismatches` Subcommand (continued)

Option	Argument	Description
`--vdcs`	*vdc1, vdc2,vdc3*	Optional. A comma-separated list of organization VDC names for which to detect or fix resource pool mismatches. If the VDC name contains a comma or a space, surround the VDC name with quotation marks.
`--pvdcs`	*pvdc1,pvdc2,pvdc3*	Optional. A comma-separated list of provider VDC names for which to detect or fix resource pool mismatches. If the VDC name contains a comma or a space, surround the VDC name with quotation marks.

Configure a Test Connection Denylist in VMware Cloud Director

After installation or upgrade, use the `manage-test-connection-denylist` command of the cell management tool to block access to internal hosts before providing tenants with access to the VMware Cloud Director network.

Starting with VMware Cloud Director 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers and to verify the server identity as part of an SSL handshake.

To protect the internal network in which a VMware Cloud Director instance is deployed from malicious attacks, system providers can configure a denylist of internal hosts that are unreachable to tenants.

This way, if a malicious attacker with tenant access attempts to use the connection testing VMware Cloud Director API to map the network in which VMware Cloud Director is installed, they won't be able to connect to the internal hosts on the denylist.

After installation or upgrade and before providing tenants with access to the VMware Cloud Director network, use the `manage-test-connection-denylist` command of the cell management tool to block tenant access to internal hosts.

Procedure

1 Log in or SSH as root to the OS of the VMware Cloud Director cell.

2 Run the command to add an entry to the denylist.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-denylist
option
```

Table 16-6. Cell Management Tool Options and Arguments, `manage-test-connection-denylist` Subcommand

Option	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--add-ip`	IPv4 or IPv6 address	Adds an IP address to the denylist.
`--add-name`	A subdomain or a fully qualified domain name for a host	Adds a subdomain or a domain name to the denylist.
`--add-range`	IPv4 or IPv6 address range in either CIDR or hyphenated format	Adds an IP address range to the denylist.
`--list`	None	Lists all the existing entries with denied access.

Configure Metrics Collection and Publishing in VMware Cloud Director

You can use the `configure-metrics` command of the VMware Cloud Director cell management tool to configure the set of metrics to collect.

VMware Cloud Director can collect metrics that provide current and historic information about the virtual machine performance and resource consumption. Use this subcommand to configure the metrics that VMware Cloud Director collects. Use the `cell-management-toolcassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository. See Configuring a Cassandra Metrics Database in VMware Cloud Director.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director cell as **root**.

2 Configure the metrics that VMware Cloud Director collects.

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config
pathname
```

Table 16-7. Cell Management Tool Options and Arguments, `configure-metrics` Subcommand

Command	Argument	Description
`--help(-h)`	None	Provides a summary of available commands in this category.
`--repository-host` (Deprecated)	Host name or IP address of KairosDB host	Deprecated. Use the `--cluster-nodes` option of the `cell-management-toolcassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository.
`--repository-port` (Deprecated)	KairosDB port to use.	Deprecated. Use the `--port` option of the `cell-management-toolcassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository.
`--metrics-confg`	path name	Path to the metrics configuration file

3 (Optional) Enable the metrics publishing by running the following command.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

Starting with VMware Cloud Director 10.2.2, the metrics publishing is deactivated by default.

Example: Configuring a Metrics Database Connection

This example configures the metrics collection as specified in the file `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --
metrics-config /tmp/metrics.groovy
```

The VMware Cloud Director metrics collection service implements a subset of the metrics collected by the vSphere Performance Manager. See the vSphere Performance Manager documentation for more information about metric names and collection parameters. The `metrics-config` file cites one or more metric names and provides collection parameters for each cited metric. For example:

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
        aggregator="AVERAGE"
    }
}
```

The following metric names are supported.

Table 16-8. Metric Names

Metric Name	Description
`cpu.usage.average`	Host view of this virtual machine's average actively used CPU as a percentage of total available. Includes all cores in all sockets.
`cpu.usagemhz.average`	Host view of this virtual machine's average actively used CPU as a raw measurement . Includes all cores in all sockets.
`cpu.usage.maximum`	Host view of this virtual machine's maximum actively used CPU as a percentage of total available. Includes all cores in all sockets.
`mem.usage.average`	Memory used by this virtual machine as a percentage of total configured memory.
`disk.provisioned.latest`	Storage space allocated to this virtual hard disk in the containing organization virtual data center.
`disk.used.latest`	Storage used by all virtual hard disks.
`disk.read.average`	Average read rate for all virtual hard disks.
`disk.write.average`	Average write rate for all virtual hard disks.

Note When a virtual machine has multiple disks, VMware Cloud Director reports metrics as an aggregate for all disks. CPU metrics are an aggregate of all cores and sockets.

For each named metric, you can specify the following collection parameters.

Table 16-9. Metrics Collection Parameters

Parameter Name	Value	Description
`currentInterval`	Integer number of seconds	The interval in seconds to use when querying for the latest available metric values for current metrics queries. The default value is `20`. VMware Cloud Directorsupports values greater than 20 only for Level 1 metrics, as defined by the vSphere Performance Manager.
`historicInterval`	Integer number of seconds	The interval in seconds to use when querying for historic metric values. The default value is `20`. VMware Cloud Director supports values greater than 20 only for Level 1 metrics, as defined by the vSphere Performance Manager.

Table 16-9. Metrics Collection Parameters (continued)

Parameter Name	Value	Description
`entity`	One of: `HOST`, `VM`	The type of VC object that the metric is available for. The default is `VM`. Not all metrics are available for all entities.
`instance`	A vSphere Performance Manager `PerfMetricId` instance identifier	Indicates whether to retrieve data for individual instances of a metric, for example, individual CPU cores, an aggregate of all instances, or both. A value of `"*"` collects all metrics, instance and aggregate. An empty string, `""` collects only the aggregate data. A specific string like `"DISKFILE"` collects data only for that instance. The default is `"*"`.
`minReportingInterval`	Integer number of seconds	Specifies a default aggregation interval in seconds to use when reporting time series data. Provides further control over reporting granularity when the granularity of the collection interval is not sufficient. The default is `0`, that is, no dedicated reporting interval.
`aggregator`	One of: `AVERAGE`, `MINIMUM`, `MAXIMUM`, `SUMMATION`	The type of aggregation to perform during the `minReportingInterval`. The default is `AVERAGE`.

Configuring a Cassandra Metrics Database in VMware Cloud Director

Use the `cassandra` command of the cell management tool to connect the cell to an optional metrics database.

VMware Cloud Director can collect metrics that provide current and historic information about virtual machine performance and resource consumption. Use this subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository. Use the `cell-management-tool configure-metrics` subcommand to tool to configure the set of metrics to collect. See Configure Metrics Collection and Publishing in VMware Cloud Director.

Data for historic metrics is stored in an Apache Cassandra database. See Install and Configure a Cassandra Database for Storing Historic Metric Data for more information about configuring optional database software to store and retrieve performance metrics.

To create a connection between VMware Cloud Director and an Apache Cassandra database, use a command line with the following form:

```
cell-management-tool cassandra options
```

Table 16-10. Cell Management Tool Options and Arguments, `cassandra` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available options for this command.
`--add-rollup`	None	Updates the metrics schema to include rolled-up metrics. See Install and Configure a Cassandra Database for Storing Historic Metric Data.
`--cluster-nodes`	*address* [, *address* ...]	Comma-separated list of Cassandra cluster nodes to use for VMware Cloud Director metrics.
`--clean`	None	Remove Cassandra configuration settings from the VMware Cloud Director database.
`--configure`	None	Configure VMware Cloud Director for use with an existing Cassandra cluster.
`--dump`	None	Dump the current connection configuration.
`--keyspace`	string	Set VMware Cloud Director key space name in Cassandra to *string*. Defaults to `vcloud_metrics`.
`--offline`	None	Cofigure Cassandra for use by VMware Cloud Director, but do not test the configuration by connection to VMware Cloud Director.
`--password`	string	Password of Cassandra database user
`--port`	integer	Port to connect to at each cluster node. Defaults to 9042.
`--ttl`	integer	Retain metrics data for *integer* days. Set *integer* to `0` to retain metrics data forever.
`--update-schema`	None	Initializes the Cassandra schema to hold VMware Cloud Director metrics data.
`--username`	string	User name of the Cassandra database user.

Example: Configuring a Cassandra Database Connection

Use a command like this, where *node1-ip*, *node2-ip*, *node3-ip*, and *node4-ip* are the IP address of the members of the Cassandra cluster. The default port (9042) is used. Metrics data is retained for 15 days.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --configure --
create-schema \
--cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \
--username admin --password 'P@55w0rd' --ttl 15
```

You must restart the cell after this command completes.

Recovering the VMware Cloud Director System Administrator Password

If you know the VMware Cloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the VMware Cloud Director system administrator password.

With the `recover-password` command of the cell management tool, a user who knows the VMware Cloud Director database username and password can recover the VMware Cloud Director system administrator password.

To recover the system administrator password, use a command line with the following form:

```
cell-management-tool recover-password options
```

Table 16-11. Cell Management Tool Options and Arguments, `recover-password` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--dbuser`	The user name of the VMware Cloud Director database user.	Must be supplied on the command line.
`--dbpassword`	The password of the VMware Cloud Director database user.	Prompted for if not supplied.

Update the Failure Status of a Task in VMware Cloud Director

Use the `fail-tasks` command of the VMware Cloud Director cell management tool to update the completion status associated with tasks that were running when the cell was deliberately shut down. You cannot use the `fail-tasks` command unless all cells have been shut down.

When you quiesce a cell using the `cell-management-tool -q` command, running tasks should terminate gracefully within a few minutes. If tasks continue to run on a cell that has been quiesced, the superuser can shut down the cell, which forces any running tasks to fail. After a shutdown that forced running tasks to fail, the superuser can run `cell-management-tool fail-tasks` to update the completion status of those tasks. Updating a task's completion status in this way is optional but helps maintain the integrity of system logs by clearly identifying failures caused by an administrative action.

To generate a list of tasks that are still running on a quiesced cell, use a command line with the following form:

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

Table 16-12. Cell Management Tool Options and Arguments, `fail-tasks` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--message` (-m)	Message text.	Message text to place in task completion status.

Example: Fail Tasks Running on the Cell

This example updates the task completion status associated with a task that was still running when the cell was shut down.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m
"administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1
Would you like to fail the tasks listed above?
```

Type **`y`** to update the task with a completion status of **`administrative shutdown`**. Type **`n`** to allow the task to continue running.

Note If multiple tasks are returned in the response, you must decide to fail all of them or take no action. You cannot choose a subset of tasks to fail.

Configure Audit Message Handling in VMware Cloud Director

Use the `configure-audit-syslog` command of the VMware Cloud Director cell management tool to configure the way the system logs audit messages.

Services in each VMware Cloud Director cell log audit messages to the VMware Cloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure VMware Cloud Director services to send audit messages to the Linux `syslog` utility in addition to the VMware Cloud Director database.

The system configuration script allows you to specify how audit messages are handled. See "Configure Network and Database Connections" in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*. The logging options you specify during system configuration are preserved in two files: `global.properties` and `responses.properties`. You can change the audit message logging configuration in both files with a cell management tool command line of the following form:

```
cell-management-toolconfigure-audit-syslog options
```

Any changes you make with this cell management tool subcommand are preserved in the cell's `global.properties` and `responses.properties` files. Changes do not take effect until you re-start the cell.

Table 16-13. Cell Management Tool Options and Arguments, `configure-audit-syslog` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--disable` (-d)	None	Deactivate logging of audit e vents to `syslog`. Log audit events only to the VMware Cloud Director database. This option unsets the values of the`audit.syslog.host` and `audit.syslog.port` properties in `global.properties` and `responses.properties`.
`--syslog-host` (-loghost)	IP address or fully-qualified domain name of the syslog server host	This option sets the value of the `audit.syslog.host` property to the specified address or fully-qualified domain name.
`--syslog-port` (-logport)	integer in the range 0-65535	This option sets the value of the `audit.syslog.port` property to the specified integer.

When you specify a value for `--syslog-host`, `--syslog-port`, or both, the command validates that the specified value has the correct form but does not test the combination of host and port for network accessibility or the presence of a running `syslog` service.

Example: Change the Syslog Server Host Name

Important Changes you make using this command are written to the global configuration file and the response file. Before you use this command, be sure that the response fine is in place (in `/opt/vmware/vcloud-director/etc/responses.properties`) and writeable. See "Protecting and Reusing the Response File" in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

To change the host to which syslog messages are sent, use a command like this one:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog
-loghost syslog.example.com
Using default port 514
```

This example assumes that the new host listens for syslog messages on the default port.

The command updates `global.properties` and `responses.properties`, but the changes do not take effect until you re-start the cell.

Configuring Email Templates in VMware Cloud Director

To manage the templates that the system uses when creating email alerts, you can use the `manage-email` command of the VMware Cloud Director cell management tool.

By default, the system sends email alerts that notify system administrators of events and conditions that are likely to require their intervention. The list of email recipients can be updated using the VMware Cloud Director API or the Web console. You can override the default email content for each kind of alert by using a cell management tool command line of the following form:

```
cell-management-tool manage-email  options
```

Table 16-14. Cell Management Tool Options and Arguments, `manage-email` Subcommand

Option	Argument	Description
`--help`	None	Provides a summary of available commands in this category.
`--delete`	template name	The name of the template to delete.
`--lookup`	template name	This argument is optional. If you do not supply it, the command returns a list of all template names.

Table 16-14. Cell Management Tool Options and Arguments, `manage-email` Subcommand (continued)

Option	Argument	Description
`--locale`	the template locale	By default, this command operates on templates in the en-US locale. To specify a different locale, use this option.
`--set-template`	path name to a file containing an updated email template	This file must be accessible on the local host and readable by the user vcloud.vcloud. For example, /tmp/my-email-template.txt

There are different allowed template names that you can use for different email notifications.

Table 16-15. VMware Cloud Director Email Notification Names

Name	Description	When the email is sent	Recipients
`VAPP_UNDEPLOY_NOTIFICATION_SUBJECT` `VAPP_UNDEPLOY_NOTIFICATION_BODY`	Alert when the vApp runtime lease is about to expire. When the lease expires, VMware Cloud Director suspends or powers off the vApp.	Before the runtime lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPP_STORAGE_NOTIFICATION_DELETE_SUBJECT` `VAPP_STORAGE_NOTIFICATION_BODY`	Alert when the vApp storage lease is about to expire. When the lease expires, VMware Cloud Director deletes the vApp.	Before the storage lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPP_STORAGE_NOTIFICATION_FLAG_SUBJECT` `VAPP_STORAGE_NOTIFICATION_BODY`	Alert when the vApp storage lease is about to expire. When the lease expires, VMware Cloud Director marks the vApp as expired.	Before the storage lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPPTEMPLATE_STORAGE_NOTIFICATION_DELETE_SUBJECT` `VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY`	Alert when the vApp template storage lease is about to expire. When the lease expires, VMware Cloud Director deletes the vApp template.	Before the storage lease of a vApp template expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp Template, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPPTEMPLATE_STORAGE_NOTIFICATION_FLAG_SUBJECT` `VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY`	Alert when the vApp template storage lease is about to expire. When the lease expires, VMware Cloud Director marks the vApp template as expired.	Before the storage lease of a vApp template expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp Template, or if the owner is a **system administrator**, the **organization administrators** receive the notification.

Table 16-15. VMware Cloud Director Email Notification Names (continued)

Name	Description	When the email is sent	Recipients
DISK_STORAGE_ALERT	Disk Storage Alert (Red Alert)	When there is low disk space on the datastore and it reaches the red threshold.	**System administrators**
DISK_STORAGE_ALERT_VDCS	Disk storage alert to provider VDCs. The email contains the list provider VDCs using the datastore that has a red alert due to low hard disk space.	When there is low disk space on the datastore and it reaches the red threshold.	**System administrators**
VM_HW_UPGRADE_INVALID_POWER_STATE VM_UPDATE_NESTED_HV_INVALID_POWER_STATE	A notification about the power state of a VM. To upgrade the virtual hardware, you must power off the VM.	When a user attempts to upgrade the hardware version of a VM.	The owner of the VM, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
FEDERATION_CERTIFICATE_SUCCESS_SUBJECT FEDERATION_CERTIFICATE_SUCCESS_BODY	Federation certificate expiration notification sent to all **organization administrators** when a certificate for an external SSO server is about to expire. It prompts the **organization administrators** to download a new certificate from the SSO server and update VMware Cloud Director.	If a federation certificate expires within 7 days from the current date.	**Organization administrators**
IPSEC_VPN_TUNNEL_ERROR IPSEC_VPN_TUNNEL_ERROR_SUMMARY	VPN tunnel Error (Red Alert)	When the VPN tunnel is not operational.	**System administrators**
IPSEC_VPN_TUNNEL_ENABLED IPSEC_VPN_TUNNEL_ENABLED _SUMMARY	VPN tunnel Enabled (Green Alert)	When the VPN tunnel is working again after not being operational.	**System administrators**

Table 16-16. Non-customizable Email Templates

Notification	When the email is sent	Recipients
Reconnected vCenter Server email alert	When a vCenter Server is reconnected.	**System administrators**
Disconnected vCenter Server email alert. The email states whether an error or a user request caused the disconnecting of the vCenter Server.	When a vCenter Server is disconnected.	**System administrators**

Table 16-16. Non-customizable Email Templates (continued)

Notification	When the email is sent	Recipients
AMQP Connection Lost email alert. Alert notifying that VMware Cloud Director is disconnected from the AMQP Server.	When the RabbitMQ stops working.	**System administrators**
Broken Database Connection email alert	When VMware Cloud Director is disconnected from the database.	**System administrators**
Restored Database Connection email alert	When VMware Cloud Director is reconnected to the database.	**System administrators**
Host Disconnected from Switch email alert	When a host gets disconnected from the available switches.	**System administrators**
Host Disconnected from Distributed Virtual Switch email alert	When a host gets disconnected from the available distributed virtual switches.	**System administrators**
LDAP Error email alert	During the synchronization with LDAP.	**System administrators**
LDAP User Sync email alert	During the renaming of an LDAP user.	**System administrators**
Site Associations Status Change email alert	The sites recently lost connection, regained connection, or are still down.	**System administrators**

Example: Update an Email Template

The following command replaces the current contents of the DISK_STORAGE_ALERT_VDCS email template with content you created in a file named `/tmp/DISK_STORAGE_ALERT_VDCS-new.txt`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-
template DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcsList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
$productName The $datastore is used by the followingProvider VDC(s): $pvdcsList
"

VCD Email notification details:
 name                       : DISK_STORAGE_ALERT_VDCS
 description                : Alert when used disk storage exceeds threshold
 config key                 : email.template.DISK_STORAGE_ALERT_VDCS.en-US
 template placeholders      : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcsList]
 template content           : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcsList
```

Finding Orphaned VMs in VMware Cloud Director

Use the `find-orphan-vms` command of the cell management tool to find references to virtual machines that are present in the vCenter database but not in the VMware Cloud Director database.

Virtual machines that are referenced in the vCenter database but not in the VMware Cloud Director database are considered orphan VMs because VMware Cloud Director cannot access them even though they may be consuming compute and storage resources. This kind of reference mismatch can arise for a number of reasons, including high-volume workloads, database errors, and administrative actions. The `find-orphan-vms` command enables an administrator to list these VMs so that they can be removed or re-imported into VMware Cloud Director. This command has provisions for specifying an alternate trust store, which might be needed if you are working with VMware Cloud Director or vCenter installations that use self-signed certificates.

Use a command with the following form:

```
cell-management-tool find-orphan-vms options
```

Table 16-17. Cell Management Tool Options and Arguments, `find-orphan-vms` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--enableVerifyHostname`	None	Enable the host name verification part of the SSL handshake.
`--host`	Required	IP address or fully-qualified domain name of the VMware Cloud Director installation to search for orphan VMs.
`--output-file`	path name or –	Full path name of the file to which the list of orphan VMs should be written. Specify a path name of – to write the list to the standard output.
`--password` (-p)	Required	VMware Cloud Director system administrator password.
`--port`	VMware Cloud Director HTTPS port.	Specify this only if you do not want this command to use the default VMware Cloud Director HTTPS port.
`--trustStore`	Full path name to a Java trust store file.	Specify this only if you do not want this command to use the default VMware Cloud Director trust store file.

Table 16-17. Cell Management Tool Options and Arguments, `find-orphan-vms` Subcommand (continued)

Option	Argument	Description
`--trustStorePassword`	Password to specified `--trustStore`	Required only if you use `--trustStore` to specify an alternate trust store file.
`--trustStoreType`	The type of the specified `--trustStore` (PKCS12, JCEKS, ...)	Required only if you use `--trustStore` to specify an alternate trust store file.
`--user` (-u)	Required	VMware Cloud Director system administrator user name.
`--vc-name`	Required	Name of vCenter to search for orphan VMs.
`--vc-password`	Required	vCenter administrator password.
`--vc-user`	Required	vCenter administrator user name.

Example: Finding Orphaned VMs

This example queries a single vCenter server. Because `--output-file` is specified as `-`, results are returned on the standard output.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vms \
 --host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --vc-user admin --
output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://
10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...)
[moref: "resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test
VMs", parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test
VMs", parent moref : "group-v30533")
```

Join or Leave the VMware Customer Experience Improvement Program

To join or leave the VMware Customer Experience Improvement Program (CEIP), you can use the `configure-ceip` subcommand of the VMware Cloud Director cell management tool.

This product participates in VMware’s Customer Experience Improvement Program (“CEIP”). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You can use the cell management tool to join or leave VMware's CEIP for this product at any time.

```
cell-management-tool configure-ceip options
```

If you prefer not to participate in VMware's CEIP for this product, run this command with the `--disable` option.

Table 16-18. Cell Management Tool Options and Arguments, `configure-ceip` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--disable`	None	Leaves the VMware Customer Experience Improvement Program.
`--enable`	None	Joins the VMware Customer Experience Improvement Program.
`--status`	None	Displays the current participation status in the VMware Customer Experience Improvement Program.

Example: Leave the VMware Customer Experience Improvement Program

Starting with version 10.4.2.1, when you deactivate CEIP, the VMware Cloud Director **Feedback** button does not appear. For the feedback button to appear again, you must activate CEIP and log in again to VMware Cloud Director.

To leave the VMware Customer Experience Improvement Program, use a command like this one and log in again to VMware Cloud Director:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --disable
Participation disabled
```

After you run this command, the system no longer sends any information to the VMware Customer Experience Improvement Program.

To confirm the current participation status in the VMware Customer Experience Improvement Program, use a command like this one:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --status
Participation disabled
```

Updating Application Configuration Settings in VMware Cloud Director

With the `manage-config` subcommand of the VMware Cloud Director cell management tool, you can update different application configuration settings such as catalog throttling activities.

Table 16-19. Cell Management Tool Options and Arguments, `manage-config` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available options with this subcommand.
`--delete` (`-d`)	None	Removes the target configuration setting.
`--lookup` (`-l`)	None	Look up the value of the target configuration setting.
`--name` (`-n`)	Configuration setting name	The name of the target configuration setting. Required with options `-d`, `-l`, and `-v`.
`--value` (`-v`)	Configuration setting value	Adds or updates the value for the target configuration setting.

For example, you can use the `manage-config` subcommand for Configuring Catalog Synchronization Throttling in VMware Cloud Director.

Configuring Catalog Synchronization Throttling in VMware Cloud Director

When you have many catalog items published to or subscribed from other organizations, to avoid overloading the system during catalog synchronizations, you can configure catalog synchronization throttling.

You can use the `manage-config` subcommand of the cell management tool to configure catalog synchronization throttling by limiting the number of library items that can be synced at the same time.

When a subscribed catalog initiates a catalog synchronization, the published catalog first downloads the library items from the vCenter Server repository to the VMware Cloud Director transfer service storage, then creates download links for the subscribed catalog. You can limit the number of library items that all published catalogs can download at the same time. You can limit the number of library items that all subscribed catalogs can sync at the same time. You can limit the number of library items that a single subscribed catalog can sync at the same time.

You can use the `manage-config` subcommand of the cell management tool to update the configuration settings for catalog throttling. For information about using the `manage-config` subcommand, see Updating Application Configuration Settings in VMware Cloud Director.

Table 16-20. Configuration Settings for Catalog Throttling

Configuration Setting	Default Value	Description
`vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit`	30	The limit of library items that all published catalogs in the VMware Cloud Director instance can download from vCenter Server to VMware Cloud Director at the same time. If the total number of published library items for downloading across the VMware Cloud Director instance is greater than this limit, the library items are divided into portions by this limit and downloaded in a sequence.
`vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit`	30	The limit of library items that all subscribed catalogs in a VMware Cloud Director instance can sync at the same time. If the total number of subscribed library items for syncing across the VMware Cloud Director instance is greater than this limit, the items are divided into portions by this limit and synced in a sequence.
`contentLibrary.item.sync.batch.size`	10	The limit of library items that a single subscribed catalog can sync at the same time. If a subscribed catalog tries to sync a number of library items that is greater than this limit, the items are divided into portions by this limit and synced in a sequence.

Example: Configuring Synchronization Throttling for Subscribed Catalogs

The following command sets a limit of five for the library items that a single subscribed catalog can sync at the same time.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
contentLibrary.item.sync.batch.size -v 5
```

If a subscribed catalog contains 13 library items, syncing the catalog is performed in three sequential portions. The first portion contains five items, the second portion contains the next five items, the last portion contains the remaining three items.

Debugging vCenter VM Discovery in VMware Cloud Director

By using the `debug-auto-import` subcommand of the cell management tool, you can investigate the reason for which the mechanism for discovering vApps skips one or more vCenter VMs.

In the default configuration, an organization VDC automatically discovers vCenter VMs that are created in the resource pools that back the VDC. See the discovering and adopting vApps information in the *VMware Cloud Director Service Provider Admin Guide*. If a vCenter VM does not appear in a discovered vApp, you can run the `debug-auto-import` subcommand against this VM or VDC.

```
cell-management-tool debug-auto-import options
```

The `debug-auto-import` subcommand returns a list of vCenter VMs and information about the possible reasons for being skipped by the discovery mechanism. The list also includes vCenter VMs that are discovered but failed to import to the organization VCD.

Table 16-21. Cell Management Tool Options and Arguments, `debug-auto-import` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--org`	Organization name	Optional. Lists information about the skipped VMs for the specified organization.
`--vm`	VM name or part of a VM name	Lists information about the skipped VMs that contain the specified VM name. Optional if the `--org` option is used.

Example: Debug vCenter VM Discovery by VM Name `test`

The following command returns information about skipped vCenter VMs across all organizations.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is already imported in vCD or is managed by vCD
2) Virtual machine is created by vCD

VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is not present in a vCD managed resource pool

VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry
```

In this example, the system output returns information about three vCenter VMs that are skipped by the discovery mechanism and whose names contain the string `test`. VM `import-test3` is an example of a VM that is discovered but failed to import to the VDC.

Regenerating MAC Addresses for Multisite Stretched Networks in VMware Cloud Director

If you associate two VMware Cloud Director sites that are configured with the same installation ID, you might encounter MAC address conflicts in stretched networks across these sites. To avoid such conflicts, you must regenerate the MAC addresses in one of the sites based on a custom seed that is different from the installation ID.

During the initial VMware Cloud Director setup, you set an installation ID. VMware Cloud Director uses the installation ID to generate MAC addresses for the virtual machine network interfaces. Two VMware Cloud Director installations that are configured with the same installation ID might generate identical MAC addresses. Duplicate MAC addresses might cause conflicts in stretched networks between two associated sites.

Before creating stretched networks between associated sites that are configured with the same installation ID, you must regenerate the MAC addresses in one of the sites by using the `mac-address-management` subcommand of the cell management tool.

```
cell-management-tool mac-address-management options
```

To generate new MAC addresses, you set a custom seed that is different from the installation ID. The seed does not overwrite the installation ID, but the database stores the latest seed as a second configuration parameter, which overrides the installation ID.

You run the `mac-address-management` subcommand from an arbitrary VMware Cloud Director member of the server group. The command runs against the VMware Cloud Director database, so you run the command once for a server group.

Important The MAC addresses regeneration requires some downtime of VMware Cloud Director. Before starting the regeneration, you must quiesce the activities on all cells in the server group.

Table 16-22. Cell Management Tool Options and Arguments, `mac-address-management` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--regenerate`	None	Deletes all MAC addresses that are not in use and generates new MAC addresses based on the current seed. If there is no a previously set seed, the MAC addresses are regenerated based on the installation ID. The MAC addresses that are in use are retained. **Note** All cells in the server group must be inactive. For information about quiescing the activities on a cell, see Managing a Cell.
`--regenerate-with-seed`	A seed number from 0 to 63	Sets a new custom seed in the database. - Deletes all MAC addresses that are not in use, and generates new MAC addresses based on the newly set seed. - The MAC addresses change to the `00:50:56:Seed:XX:YY` format. - VMware Cloud Director retains the MAC addresses that are in use. - The installation ID does not change. **Note** All cells in the server group must be inactive. For information about quiescing the activities on a cell, see Managing a Cell.
`--show-seed`	None	Returns the current seed and the number of MAC addresses that are in use for each seed.

Important The MAC addresses that are in use are retained. To change a MAC address that is in use to a regenerated MAC address, you must reset the network interface MAC address. For information about editing virtual machine properties, see the *VMware Cloud Director Tenant Guide*.

Example: Regenerating the MAC Addresses Based on a New Custom Seed

The following command sets the current seed to *9* and regenerates all MAC addresses that are not use based on the newly set seed:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --
regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

Example: Viewing the Current Seed and the Number of MAC Addresses in Use for Each Seed

The following command returns information about the current seed and number of MAC addresses per seed:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --
show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by     12 MAC addresses
MAC address seed    1 is in use by      1 MAC addresses
```

In this example, the system output shows that the current seed is 9, based on which there are 12 MAC addresses. In addition, there is one MAC address that is based on a previous seed or installation ID of 1.

Activate a Lazy Resource Apportioning for an Elastic Flex Organization VDC in VMware Cloud Director

Starting with VMware Cloud Director 10.5.1.1, for an elastic Flex organization VDC, you can activate a setting for reconfiguration of the resource pools backing the VDC only when necessary.

In earlier VMware Cloud Director releases, the memory and CPU resources are allocated proportionally to the number of virtual machines (VMs) residing in the resource pools backing the Flex organization VDC. Every time you create or power on a new VM, VMware Cloud Director triggers a reconfiguration of the allocated resources in the resource pools.

Starting with VMware Cloud Director 10.5.1.1, you can set up resource pool reconfiguration to occur only when the resource pool lacks the necessary resources for the specified VM operation. To activate this setting, you must set the `vcloud.flex.vdc.lazy.resource.apportioning.enabled` parameter to `true`.

Procedure

1 Log in or SSH as **`root`** to the OS of any of the VMware Cloud Director cells.

2 To activate the lazy resource apportioning, run the command.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.flex.vdc.lazy.resource.apportioning.enabled -v true
```