# Contents

vCloud Director Administrator's Guide 6

Updated Information 7

## 1 Getting Started with vCloud Director 8
- Overview of vCloud Director Administration 9
- Log In to the Web Console 11
- System Administrator Home Page 12
- Preparing the System 12
- Replace SSL Certificates 13
- Set User Preferences 13
- Install Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 13
- Length Limits on Names and Descriptions 14

## 2 Adding Resources to vCloud Director 16
- Adding vSphere Resources 16
- Adding Cloud Resources 19

## 3 Creating and Provisioning Organizations 26
- Understanding Leases 26
- Understanding Allocation Models 27
- Create an Organization 29
- Allocate Resources to an Organization 34

## 4 Working With Catalogs 43
- Add a New Catalog 44
- Access a Catalog 46
- Share A Catalog 46
- Publish a Catalog to an External Organization 47
- Change the Owner of a Catalog 48
- Delete a Catalog 48
- Change the Properties of a Catalog 48
- Subscribe to an External Catalog Feed 49

## 5 Managing Cloud Resources 51
- Managing Provider Virtual Datacenters 51
- Managing Organization Virtual Datacenters 59
- Managing Organization Virtual Data Center Templates 72
Managing External Networks  
Managing Edge Gateways  
Managing Organization Virtual Datacenter Networks  
Managing Network Pools  
Managing Cloud Cells  
Managing Service Offerings  
Configuring and Managing Multisite Deployments  
Create or Update Object Metadata

6 Managing vSphere Resources  
Managing vCenter Servers  
Managing vSphere ESXi Hosts  
Creating and Managing VM-Host Affinity Rules  
Discovering and Adopting vApps  
Managing vSphere Datastores  
Managing Stranded Items  
View Resource Pool Properties  
View Storage Policy Properties

7 Managing Organizations  
Enable or Disable an Organization  
Delete an Organization  
Add a Catalog to an Organization  
Editing Organization Properties  
Managing Organization Resources  
Managing Organization vApps and Virtual Machines  
Migrate Tenant Storage

8 Managing System Administrators and Roles  
Add a System Administrator  
Import a System Administrator  
Enable or Disable a System Administrator  
Delete a System Administrator  
Edit System Administrator Profile and Contact Information  
Send an Email Notification to Users  
Delete a System Administrator Who Lost Access to the System  
Import a Group  
Delete an LDAP Group  
View Group Properties  
Working With Roles and Rights
9 Managing System Settings 179
  Modify General System Settings 179
  General System Settings 179
  Editing System Email Settings 181
  Configuring Blocking Tasks and Notifications 182
  Configuring System LDAP Settings 184
  Customize the vCloud Director Client UI 187
  Configuring Public Addresses 189
  Configure System Limits 190
  Configure the Account Lockout Policy 190
  Configure vCloud Director to use the vSphere SSO SAML provider 191

10 Monitoring vCloud Director 193
  Viewing Tasks and Events 193
  Monitor and Manage Blocking Tasks 195
  View Usage Information for a Provider Virtual Datacenter 196
  View Usage Information for an Organization Virtual Datacenter 196
  Using vCloud Director's JMX Service 196
  Viewing the vCloud Director Logs 197
  vCloud Director and Cost Reporting 198

11 Cell Management Tool Reference 199
  Managing a Cell 202
  Managing Cell Applications 204
  Exporting Database Tables 205
  Detecting and Repairing Corrupted Scheduler Data 208
  Generating Self-Signed Certificates for the HTTP and Console Proxy Endpoints 209
  Replacing Certificates for the HTTP and Console Proxy Endpoints 210
  Importing SSL Certificates from External Services 212
  Managing the List of Allowed SSL Ciphers 213
  Managing the List of Allowed SSL Protocols 215
  Configuring Metrics Collection 217
  Configuring a Cassandra Metrics Database 219
  Recovering the System Administrator Password 221
  Update the Failure Status of a Task 221
  Configure Audit Message Handling 222
  Updating the Database Connection Properties 223
  Configure a vCloud Director Installation 226
  Configure Email Templates 228
  Finding Orphaned VMs 229
  Join or Leave the VMware Customer Experience Improvement Program 231
  Migrate to a PostgreSQL Database 232
vCloud Director Administrator’s Guide

The VMware vCloud Director Administrator’s Guide provides information to the vCloud Director system administrator about how to add resources to the system, create and provision organizations, manage resources and organizations, and monitor the system.

Intended Audience

This book is intended for anyone who wants to configure and manage a vCloud Director installation. The information in this book is written for experienced system administrators who are familiar with Linux, Windows, IP networks, and VMware vSphere.
Updated Information

This vCloud Director Administrator's Guide is updated with each release of the product or when necessary.

This table provides the update history of the vCloud Director Administrator's Guide.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09 JAN 2019</td>
<td>Added an Important note to Step 5 in Create a Provider Virtual Datacenter and to Add a VM Storage Policy to a Provider Virtual Data Center.</td>
</tr>
<tr>
<td>04 MAY 2018</td>
<td>Updated topics Updating the Database Connection Properties and Migrate to a PostgreSQL Database to improve the information about using the reconfigure-database and dbmigrate subcommands of the cell management tool.</td>
</tr>
<tr>
<td>29 JAN 2018</td>
<td>■ Updated the Prerequisites section of topic Add a Network Pool Backed by vSphere Port Groups.</td>
</tr>
<tr>
<td></td>
<td>■ Updated the Prerequisites section of topic Add an External Network.</td>
</tr>
<tr>
<td>29 NOV 2017</td>
<td>■ Updated the Prerequisites section of topic Migrate Tenant Storage.</td>
</tr>
<tr>
<td></td>
<td>■ Added an Important note to topic Enable VAAI for Fast Provisioning on a Datastore.</td>
</tr>
<tr>
<td></td>
<td>■ Added an Important note to topic Fast Provisioning of Virtual Machines.</td>
</tr>
<tr>
<td></td>
<td>■ Retitled and updated the procedure in topic Configure vCloud Director to use the vSphere SSO SAML provider.</td>
</tr>
<tr>
<td>28 SEP 2017</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Getting Started with vCloud Director

The first time you log in to the vCloud Director Web console, the Home tab guides you through the steps to configure your installation.

- **Overview of vCloud Director Administration**
  VMware vCloud Director is a software product that provides the ability to build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual datacenters and exposing them to users through Web-based portals and programmatic interfaces as a fully-automated, catalog-based service.

- **Log In to the Web Console**
  You can access the vCloud Director user interface by using a Web browser.

- **System Administrator Home Page**
  The Home tab provides links to common tasks and support resources.

- **Preparing the System**
  The Home tab in the vCloud Director Web console provides links to the tasks required to prepare the system for use. Links become active after you complete prerequisite tasks.

- **Replace SSL Certificates**
  If any members of your vCloud Director server group are using self-signed SSL certificates, you can upgrade them to signed SSL certificates to obtain a higher level of trust within your cloud.

- **Set User Preferences**
  You can set certain display and system alert preferences that take effect every time you log in to the system. You can also change the password for your system administrator account.

- **Install Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files**
  Install Java Cryptography Extension (JCE) unlimited strength jurisdiction files to remove restrictions on cryptographic strength that can prevent users from successfully logging in to vCloud Director using vSphere Sign On.

- **Length Limits on Names and Descriptions**
  Follow these guidelines when entering values in vCloud Director.
Overview of vCloud Director Administration

VMware vCloud Director is a software product that provides the ability to build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual datacenters and exposing them to users through Web-based portals and programmatic interfaces as a fully-automated, catalog-based service.

The VMware vCloud Director Administrator's Guide provides information about adding resources to the system, creating and provisioning organizations, managing resources and organizations, and monitoring the system.

vSphere Resources

vCloud 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. vCloud Director also utilizes vSphere distributed switches and vSphere port groups to support virtual machine networking.

You can use these underlying vSphere resources to create cloud resources.

Cloud Resources

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

Cloud resources include provider and organization virtual datacenters, external networks, organization virtual datacenter networks, and network pools. Before you can add cloud resources to vCloud Director, you must add vSphere resources.

Provider Virtual Datacenters

A provider virtual datacenter 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.

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

Organization Virtual Datacenters

An organization virtual datacenter provides resources to an organization and is partitioned from a provider virtual datacenter. Organization virtual datacenters 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 datacenters.
vCloud Director Networking

vCloud Director supports three types of networks.

- External networks
- Organization virtual datacenter networks
- vApp networks

Some organization virtual datacenter 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 datacenter networks can connect to external networks to provide Internet connectivity to virtual machines inside of a vApp.

Only system administrators create and manage external networks.

Organization Virtual Datacenter Networks

An organization virtual datacenter network is contained within a vCloud Director organization virtual datacenter and is available to all the vApps in the organization. An organization virtual datacenter network allows vApps within an organization to communicate with each other. You can connect an organization virtual datacenter network to an external network to provide external connectivity. You can also create an isolated organization virtual datacenter network that is internal to the organization. Certain types of organization virtual datacenter networks are backed by network pools.

Only system administrators can create organization virtual datacenter networks. System administrators and organization administrators can manage organization virtual datacenter networks, although there are some limits to what an organization administrator can do.

vApp Networks

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

Most users with access to a vApp can create and manage their own vApp networks. Working with vApp networks is described in the *VMware vCloud Director User's Guide*. 
Network Pools

A network pool is a group of undifferentiated networks that is available for use within an organization virtual datacenter. A network pool is backed by vSphere network resources such as VLAN IDs or port groups. vCloud Director uses network pools to create NAT-routed and internal organization virtual datacenter 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 datacenter in vCloud Director can have one network pool. Multiple organization virtual datacenters can share the same network pool. The network pool for an organization virtual datacenter provides the networks created to satisfy the network quota for an organization virtual datacenter.

Only system administrators can create and manage network pools.

Organizations

vCloud Director supports multi-tenancy through the use of 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 administrator tasks are described in the *VMware vCloud Director User’s Guide*.

Users and Groups

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

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 catalog's 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. Organizations administrators can then choose which catalog items to provide to their users.

Log In to the Web Console

You can access the vCloud Director user interface by using a Web browser.

For a list of supported browsers, see the *VMware vCloud Director Installation and Configuration Guide*.
Prerequisites

You must have the system administrator user name and password that you created during the system setup.

Procedure

1. Open a Web browser and navigate to https://hostname.domain.tld/cloud.
   
   For hostname.domain.tld, provide the fully qualified domain name associated with the primary IP address of the vCloud Director server host. For example, https://cloud.example.com/cloud.

2. Type the system administrator user name and password and click Login.

   vCloud Director displays a list of the next tasks you should perform.

System Administrator Home Page

The Home tab provides links to common tasks and support resources.

The first time you log in after installing vCloud Director, the Home tab includes a list of quick start tasks, designed to help you get the system up and running. You can continue to access these tasks even after the system is configured.

The Home tab also includes links to many of the most common tasks related to managing cloud resources, organizations, and system users.

Preparing the System

The Home tab in the vCloud Director Web console provides links to the tasks required to prepare the system for use. Links become active after you complete prerequisite tasks.

For more information about each task, see Table 1-1.

Table 1-1. Quick Start Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach a vCenter</td>
<td>Attach a vCenter Server</td>
</tr>
<tr>
<td>Create a Provider Virtual Datacenter</td>
<td>Create a Provider Virtual Datacenter</td>
</tr>
<tr>
<td>Create an External Network</td>
<td>Add an External Network</td>
</tr>
<tr>
<td>Create a Network Pool</td>
<td>Network Pools</td>
</tr>
<tr>
<td>Create an Organization</td>
<td>Create an Organization</td>
</tr>
<tr>
<td>Allocate Resources to an Organization</td>
<td>Create an Organization Virtual Datacenter</td>
</tr>
<tr>
<td>Add a Network to an Organization</td>
<td>Adding Networks to an Organization Virtual Datacenter</td>
</tr>
<tr>
<td>Add a Catalog to an Organization</td>
<td>Add a Catalog to an Organization</td>
</tr>
</tbody>
</table>
Replace SSL Certificates

If any members of your vCloud Director server group are using self-signed SSL certificates, you can upgrade them to signed SSL certificates to obtain a higher level of trust within your cloud.

You can use the cell management tool (CMT) certificates subcommand to upgrade the SSL certificates on a vCloud Director server. See Replacing Certificates for the HTTP and Console Proxy Endpoints for details.

Each vCloud Director server requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. You must run the CMT utility for each member of your vCloud Director server group. You can use signed certificates (signed by a trusted certification authority) or self-signed certificates. Signed certificates provide the highest level of trust.

Set User Preferences

You can set certain display and system alert preferences that take effect every time you log in to the system. You can also change the password for your system administrator account.

Procedure

1. In the title bar of the Web console, click Preferences.
2. Click the Defaults tab.
3. Select the page to display when you log in.
4. Select the number of days or hours before a runtime lease expires that you want to receive an email notification.
5. Select the number of days or hours before a storage lease expires that you want to receive an email notification.
6. Click the Change Password tab.
7. (Optional) Type your current password and type your new password twice.
8. Click OK.

Install Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files

Install Java Cryptography Extension (JCE) unlimited strength jurisdiction files to remove restrictions on cryptographic strength that can prevent users from successfully logging in to vCloud Director using vSphere Sign On.

Because of import control restrictions of some countries, the JCE policy files included in vCloud Director support an encryption strength that is insufficient for some applications, including the SAML identity provider.
Prerequisites

You must have superuser credentials for each cell.

Procedure

1. Download the policy files for the version of Java installed on the cell. This release of vCloud Director uses Java version 8. You can download the Java Cryptography Extension unlimited strength jurisdiction files for Java 8 from http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html.

2. For each cell in your installation, take the following steps, as documented in the vCloud Director Installation and Upgrade Guide:
   
a. Use the cell management tool to quiesce the cell.
   
b. Stop vCloud Director services on the cell.
   
c. Locate the JRE policy files in the $VCLOUD_HOME/jre directory and replace them with the downloaded policy files, preserving the ownership and permissions of the replaced files.
   
d. Re-start vCloud Director services on the cell.

What to do next

Repeat this procedure for all cells.

Length Limits on Names and Descriptions

Follow these guidelines when entering values in vCloud 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>
<thead>
<tr>
<th>Object</th>
<th>Property</th>
<th>Maximum Length in Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog</td>
<td>name</td>
<td>128</td>
</tr>
<tr>
<td>Catalog</td>
<td>Description</td>
<td>256</td>
</tr>
<tr>
<td>EdgeGateway</td>
<td>name</td>
<td>35</td>
</tr>
<tr>
<td>Media</td>
<td>name</td>
<td>128</td>
</tr>
<tr>
<td>Media</td>
<td>Description</td>
<td>256</td>
</tr>
<tr>
<td>VApp</td>
<td>name</td>
<td>128</td>
</tr>
<tr>
<td>VApp</td>
<td>Description</td>
<td>256</td>
</tr>
<tr>
<td>VAppTemplate</td>
<td>name</td>
<td>128</td>
</tr>
<tr>
<td>VAppTemplate</td>
<td>Description</td>
<td>256</td>
</tr>
<tr>
<td>Vdc</td>
<td>name</td>
<td>256</td>
</tr>
<tr>
<td>Vdc</td>
<td>Description</td>
<td>256</td>
</tr>
<tr>
<td>Object</td>
<td>Property</td>
<td>Maximum Length in Characters</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Vm</td>
<td>name</td>
<td>128</td>
</tr>
<tr>
<td>Vm</td>
<td>ComputerName</td>
<td>15 on Windows, 63 on all other platforms</td>
</tr>
</tbody>
</table>
Adding Resources to vCloud Director

vCloud Director derives its resources from an underlying vSphere virtual infrastructure. After you register vSphere resources in vCloud Director, you can allocate these resources for organizations within the vCloud Director installation to use.

This chapter includes the following topics:

- Adding vSphere Resources
- Adding Cloud Resources

Adding vSphere Resources

vCloud 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.

For information about vCloud Director system requirements and supported versions of vCenter Server and ESXi see the *VMware vCloud Director Installation and Configuration Guide*.

Attach a vCenter Server

Attach a vCenter Server to make its resources available for use with vCloud Director. After you attach a vCenter Server, you can assign its resource pools, datastores, and networks to a provider virtual datacenter.

**Prerequisites**

An instance of VMware NSX™ is installed and configured for vCloud Director. For more information, see the *VMware vCloud Director Installation and Configuration Guide*.

**Procedure**

1. **Open the Attach New vCenter Wizard**
   
   Open the Attach New vCenter wizard to start the process of attaching a vCenter Server to vCloud Director.

2. **Provide vCenter Server Connection and Display Information**
   
   To attach a vCenter Server to vCloud Director, you must provide connection information and a display name for the vCenter Server.
3 Connect to NSX Manager

VMware vCloud Director requires VMware NSX ™ to provide network services. Each VMware vCenter™ you attach to vCloud Director requires its own instance of NSX manager.

4 Confirm Settings and Attach the vCenter Server

Before you attach the new vCenter Server, review the settings you entered.

Open the Attach New vCenter Wizard

Open the Attach New vCenter wizard to start the process of attaching a vCenter Server to vCloud Director.

Procedure

1 Click the Manage & Monitor tab and then click vCenters in the left pane.

2 Click the Attach New vCenter button.

   The Attach New vCenter wizard launches.

Provide vCenter Server Connection and Display Information

To attach a vCenter Server to vCloud Director, you must provide connection information and a display name for the vCenter Server.

Procedure

1 Type the host name or IP address of the vCenter Server.

2 Select the port number that vCenter Server uses.

   The default port number is 443.

3 Type the user name and password of a vCenter Server administrator.

   The user account must have the Administrator role in vCenter.

4 Type a name for the vCenter Server.

   The name you type becomes the display name for the vCenter Server in vCloud Director.

5 (Optional) Type a description for the vCenter Server.

6 Click Next to save your choices and go to the next page.

Connect to NSX Manager

VMware vCloud Director requires VMware NSX ™ to provide network services. Each VMware vCenter™ you attach to vCloud Director requires its own instance of NSX manager.

Procedure

1 Type the host name or IP address of the NSX manager instance to use with the vCenter Server that you are attaching.
2 Type the user name and password to connect to NSX.
   The default user name is `admin` and the default password is `default`. You can change these defaults in the NSX user interface.

3 Click **Next** to save your choices and go to the next page.

**Confirm Settings and Attach the vCenter Server**

Before you attach the new vCenter Server, review the settings you entered.

**Procedure**

1 Review the settings for the vCenter Server and NSX Manager.

2 (Optional) Click **Back** to modify the settings.

3 Click **Finish** to accept the settings and attach the vCenter Server.

The system attaches the new vCenter Server and registers its resources for provider virtual datacenters to use.

**What to do next**

Assign an NSX Manager license key in the vCenter Server.

**Assign the NSX License Key in vCenter**

After you attach a vCenter Server to vCloud Director you must use the vSphere Client to assign a license key for the NSX Manager that supports vCloud Director networking.

**Prerequisites**

This operation is restricted to system administrators.

**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 vCloud Director. You can use this license key in multiple vCenter Servers.

6 Click **OK**.
Adding Cloud Resources

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

Cloud resources include provider and organization virtual datacenters, external networks, organization virtual datacenter networks, and network pools. Before you can add cloud resources to vCloud Director, you must add vSphere resources.

For more information about organization virtual datacenters, see Allocate Resources to an Organization.
For more information about organization virtual datacenter networks, see Managing Organization Virtual Datacenter Networks

Provider Virtual Datacenters

A provider virtual datacenter (Provider VDC) combines the compute and memory resources of a single vCenter Server resource pool with the storage resources of one or more storage policies created on that vCenter Server.

A typical vCloud Director system includes multiple Provider VDCs configured to meet various service level requirements. Each Provider VDC must be configured with a primary resource pool. Additional resource pools from the same vCenter Server can be added as needed. Non-primary resource pools can also be removed to free up vSphere resources for use in other Provider VDCs. The primary resource pool cannot be removed.

If you plan to add a resource pool that is part of a cluster that uses vSphere HA, make sure you are familiar with how vSphere HA calculates slot size. For more information about slot sizes and customizing vSphere HA behavior, see the VMware vSphere Availability Guide.

Create a Provider Virtual Datacenter

A system administrator must create a provider virtual datacenter (Provider VDC) to make vSphere compute, memory, and storage resources available to vCloud Director.

A system administrator must create a Provider VDC and the organization VDCs that consume its resources before any organization can begin deploying VMs or creating catalogs. The relationship of Provider VDCs to the organization VDCs they support is an administrative decision that 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, think about 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, but 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 Provider VDC.

- Capabilities such as IOPS support and VM-Host affinity rules require underlying support configured in the vCenter Server that backs the Provider VDC (see Configure Storage I/O Control Support in a Provider VDC and Creating and Managing VM-Host Affinity Rules).

- 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.

- You can create resource pools backed by vSphere clusters that are optimally configured for hosting NSX edges that have VLAN uplinks, then use vCloud Director metadata to indicate that the system should 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

- This operation is restricted to system administrators.

- Verify that at least one vCenter Server is attached and has a resource pool with available capacity in a cluster configured to use automated DRS. The vCenter Server must have the NSX license key.

- Set up the VXLAN infrastructure in NSX Manager. See the 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 VXLAN-Backed Network Pool for an NSX Transport Zone.

Procedure

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.

2. Click New Provider VDC.

3. Type a name and optional description for the Provider VDC.

   You can use these fields to indicate the vSphere functions available to organization VDCs backed by this Provider VDC, for example, vSphere HA or storage policies with IOPS support. Select Enabled to enable the Provider VDC upon creation.

   Click Next to save your changes and continue.

4. Select a vCenter Server and resource pool to serve as the primary resource pool for this Provider VDC.

   This page lists vCenter Servers registered to vCloud Director. Click a vCenter Server to show its available resource pools. If no resource pools are shown for a vCenter Server, use the vSphere client to create a new resource pool on that server.

   Click Next to save your changes and continue.
5 Add a storage policy.

All vSphere storage policies supported by the resource pool you selected in Step 4 are listed. Select one or more storage policies for the Provider VDC to support and click Add.

**Important** vCloud Director does not support VM storage policies for host-based data services such as encryption and storage I/O control.

Click **Next** to save your changes and continue.

6 Configure the VXLAN network pool for this Provider VDC.

Every Provider VDC must have a VXLAN network pool. You can have the system create one for you with a default scope, or you can use a custom VXLAN pool based on a specific NSX transport zone.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a VXLAN pool that the system created for you</td>
<td>Select Create a default VXLAN Network Pool and click Next.</td>
</tr>
<tr>
<td>Use a custom VXLAN pool is based on a specific NSX transport zone.</td>
<td>Select Select VXLAN Network Pool from list. Choose a network pool from the list and click Next.</td>
</tr>
</tbody>
</table>

7 Select the highest virtual hardware version you want the Provider VDC to support.

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.

Click **Next** to save your changes and continue.

8 Review your choices and click **Finish** to create the Provider VDC.

**What to do next**

Consider creating additional resource pools and adding them to this Provider VDC. Adding one or more secondary resource pools enables the Provider VDC to provide specialized capabilities (such as Edge clusters, affinity groups, and hosts with special configurations) that might be required by some organizations. See Add a Resource Pool to a Provider VDC.

**External Networks**

A vCloud Director external network provides an uplink interface that connects networks and VMs in the system to a network outside of the system, such as a VPN, a corporate intranet, or the public Internet. An external network must be created by the system administrator, and can be backed by one or more vSphere networks.
If you have more than one vCenter server registered to the system, you can create multiple external networks, each backed by a vSphere network. You can also create external networks that are backed by multiple vSphere networks, one from each of your vCenter servers. This approach can simplify IP address management in vCloud Director. You can modify the properties of an external network to change its network backings.

**External Networks Backed by A Single vSphere Network**

When an external network is backed by a single vSphere network, the system administrator must manage allocation of IP addresses used by consumers of the external network in all organizations. This requires manually configuring IP ranges on the underlying VLAN to provide each consumer of the external network with a non-overlapping set of IP addresses on the vSphere network.

**External Networks Backed by Multiple vSphere Networks**

An external network can be backed by multiple vSphere networks, subject to several constraints.

- The network can have at most one backing vSphere network on each vCenter server registered to the system.
- Backing network switches must all be of the same type, either DVSwitch or Standard switch.

**Add an External Network**

Add an external network to register vSphere network resources for vCloud Director to use. You can create organization VDC networks that connect to an external network.

**Prerequisites**

A vSphere port group is available. Port groups with or without VLAN trunking are supported. VMware recommends using an elastic port group with static port binding.

**Procedure**

1. Click the Manage & Monitor tab and click External Networks in the left pane.
2. Click the Add Network button.
3. Select a vCenter server and vSphere network and click Add.
4. (Optional) If multiple vCenter servers are listed, select another vCenter server and vSphere network and click Add.
   
   All of the vSphere networks you add must originate on the same type of switch: either DVSwitch or Standard switch. You can select only one vSphere network from each vCenter server.
5. When you have finished adding backing vCenter servers and vSphere networks, click Next.
6. Type the network settings and click Next.
7. Type a name and optional description for the network and click Next.
8. Review the network settings and click Finish.
What to do next

You can now create an organization virtual datacenter network that connects to the external network.

Network Pools

A network pool is a group of undifferentiated networks that is available for use in an organization virtual datacenter to create vApp networks and certain types of organization virtual datacenter networks.

A network pool is backed by vSphere network resources such as VLAN IDs or port groups. vCloud Director uses network pools to create NAT-routed and internal organization virtual datacenter 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 datacenter in vCloud Director can have one network pool. Multiple organization virtual datacenters can share the same network pool. The network pool for an organization virtual datacenter provides the networks created to satisfy the network quota for an organization virtual datacenter.

A VXLAN network pool is created when you create a provider virtual datacenter. In most cases, this is the only network pool you will need.

VXLAN Network Pools

Every Provider VDC includes a VXLAN network pool.

This pool is given a name derived from the name of the containing provider virtual datacenter 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.

vCloud Director VXLAN networks are based on the IETF VXLAN standard, and provide the following 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 vCloud Director environment, see the NSX Administration Guide.

Create a VXLAN-Backed Network Pool for an NSX Transport Zone

You can add a VXLAN-backed network pool to register an NSX transport zone for vCloud Director to use.

Prerequisites

Create an NSX transport zone on any vCenter Server registered to vCloud Director. See the NSX Administration Guide.
Procedure
1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Click Add Network Pool.
3. Select VXLAN-backed and click Next.
4. Select a vCenter Server and NSX transport zone and click Next.
5. Type a name and optional description for the network pool and click Next.
6. Review the network pool settings and click Finish.

Add a Network Pool That Is Backed by VLAN IDs
You can add a VLAN-backed network pool to register vSphere VLAN IDs for vCloud Director to use. A VLAN-backed network pool provides the best security, scalability, and performance for organization virtual datacenter 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 properly isolate the VLANs can cause a disruption on the network.

Procedure
1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Click Add Network Pool.
3. Select VLAN-backed and click Next.
4. Type a range of VLAN IDs and click Add.
   You can create one network for each VLAN ID.
5. Select a vCenter Server and vSphere distributed switch and click Next.
6. Type a name and optional description for the network and click Next.
7. Review the network pool settings and click Finish.

What to do next
You can now create an organization virtual datacenter network that is backed by the network pool or associate the network pool with an organization virtual datacenter and create vApp networks.
Add a Network Pool Backed by vSphere Port Groups

You can add a network pool backed by port groups to register vSphere port groups for vCloud Director to use. 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 properly isolate the port groups can cause network disruption.

**Prerequisites**

Verify that one or more port groups are available in vSphere. The port groups must be available on each ESXi host in the cluster, and each port group must use only a single VLAN. Port groups with or without VLAN trunking are supported.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
2. Click **Add Network Pool**.
3. Select **vSphere Port Group-backed** and click **Next**.
4. Select a vCenter Server and click **Next**.
5. Select one or more port groups, click **Add**, and click **Next**.
   - You can create one network for each port group.
6. Type a name and optional description for the network and click **Next**.
7. Review the network pool settings and click **Finish**.

**What to do next**

You can now create an organization virtual datacenter network that the network pool backs, or associate the network pool with an organization virtual datacenter and create vApp networks.
Creating and Provisioning Organizations

Organizations provide resources to a group of users and set policies that determine how users can consume those resources. Create an organization for each group of users that requires its own resources, policies, or both.

This chapter includes the following topics:

- Understanding Leases
- Understanding Allocation Models
- Create an Organization
- Allocate Resources to an Organization

Understanding Leases

Creating an organization involves specifying leases. Leases provide a level of control over an organization’s storage and compute resources by specifying the maximum amount of time that vApps can be running and that vApps and vApp templates can be stored.

The goal of a runtime lease is to prevent inactive vApps from consuming compute resources. For example, if a user starts a vApp and goes on vacation without stopping it, the vApp continues to consume resources.

A runtime lease begins when a user starts a vApp. When a runtime lease expires, vCloud Director stops the vApp.

The goal of a storage lease is to prevent unused vApps and vApp templates from consuming storage resources. A vApp storage lease begins when a user stops the vApp. Storage leases do not affect running vApps. A vApp template storage lease begins when a user adds the vApp template to a vApp, adds the vApp template to a workspace, downloads, copies, or moves the vApp template.

When a storage lease expires, vCloud Director marks the vApp or vApp template as expired, or deletes the vApp or vApp template, depending on the organization policy you set.

For more information about specifying lease settings, see Configure Organization Lease, Quota, and Limit Settings.

Users can configure email notification to receive a message before a runtime or storage lease expires. See Set User Preferences for information about lease expiration preferences.
**Understanding Allocation Models**

An allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

**Allocation Pool Allocation Model**

With the allocation pool allocation model, a percentage of the resources you allocate from the provider virtual datacenter are committed to the organization virtual datacenter. 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.

Starting with vCloud Director 5.1.2, system administrators can configure allocation-pool organization virtual datacenters to be elastic or non-elastic. This is a global setting that affects all allocation-pool organization virtual datacenters. See Modify General System Settings.

By default, allocation-pool organization virtual datacenters have a elastic allocation pool enabled. Systems upgraded from vCloud Director 5.1 that have allocation-pool organization virtual datacenters with virtual machines spanning multiple resource pools have elastic allocation pool enabled by default.

When allocation-pool virtual datacenters have the elastic allocation pool feature enabled, the organization virtual datacenter spans and uses all resource pools associated with its provider virtual datacenter. 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 a sufficient number of virtual machines can be deployed on the organization virtual datacenter without CPU being a bottleneck factor.

When a virtual machine is created, the placement engine places it on a provider virtual datacenter resource pool that best fits the requirements of the virtual machine. A subresource pool is created for this organization virtual datacenter under the provider virtual datacenter resource pool, and the virtual machine is placed under that subresource pool.

When the virtual machine powers on, the placement engine checks the provider virtual datacenter 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 virtual datacenter resource pool with sufficient resources to run the virtual machine. A subresource pool for the organization virtual datacenter is created if one does not already exist.

The subresource pool is configured with sufficient resources to run the new virtual machine. The subresource pool's memory limit is increased by the virtual machine's configured memory size, and its memory reservation is increased by the virtual machine's configured memory size times the percentage guarantee factor for the organization virtual datacenter. 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 virtual datacenter level. The CPU reservation is increased by the number of vCPU configured for the virtual machine times the vCPU specified at the organization virtual datacenter level times the percentage guarantee factor for CPU set at the organization virtual datacenter 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 virtual datacenter resource pool.
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 virtual datacenter.

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 disabled, the behavior of allocation-pool organization virtual datacenters is similar to the allocation pool model in vCloud Director 1.5. In this model, the vCPU frequency is not configurable. Overcommitment is controlled by setting the percentage of resources guaranteed.

**Pay-As-You-Go Allocation Model**

With the pay-as-you-go allocation model, resources are committed only when users create vApps in the organization virtual datacenter. You can specify a percentage of resources to guarantee, which allows you to overcommit resources. You can make a pay-as-you-go organization virtual datacenter elastic by adding multiple resource pools to its provider virtual datacenter.

Resources committed to the organization are applied at the virtual machine level.

When a virtual machine is powered on, the placement engine checks the resource pool and assigns it to another resource pool if the original resource pool cannot accommodate the virtual machine. If a sub-resource pool is not available for the resource pool, vCloud 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 is placed, and the virtual machine placement engine places the virtual machine on a provider virtual datacenter resource pool.

The benefit of the pay-as-you-go model is that it can take advantage of new resources added to the provider virtual datacenter.

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 aren’t 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.

**Reservation Pool Allocation Model**

All of the resources you allocate are immediately committed to the organization virtual datacenter. Users in the organization can control 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 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 virtual datacenter on the primary cluster, the organization virtual datacenter creation fails.

Other limitations of this model are that it is not elastic and organization users might set nonoptimal shares, rates, and limits on virtual machines, leading to underuse of resources.

Create an Organization

Creating an organization involves specifying the organization settings and creating a user account for the organization administrator.

Procedure

1. **Open the New Organization Wizard**
   - Open the New Organization wizard to start the process of creating an organization.

2. **Name the Organization**
   - Provide a descriptive name and an optional description for your new organization.

3. **Specify the Organization LDAP Options**
   - You can use an LDAP service to provide a directory of users and groups for the organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. Only a system administrator can set LDAP options. An organization administrator cannot modify LDAP options.

4. **Add Local Users to the Organization**
   - Every organization should have at least one local organization administrator account, so that users can log in even if the LDAP and SAML services are unavailable.

5. **Set the Organization Catalog Sharing, Publishing, and Subscription Policies**
   - Catalogs provide organization users with catalogs of vApp templates and media that they can use to create vApps and install applications on virtual machines.

6. **Configure Email Preferences**
   - vCloud Director requires an SMTP server to send user notification and system alert emails. An organization can use the system email settings or use its own email settings.

7. **Configure Organization Lease, Quota, and Limit Settings**
   - Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. Use these settings to prevent users from depleting or monopolizing an organization’s resources.
8 Confirm Settings and Create the Organization

Before you create the organization, review the settings you entered.

Open the New Organization Wizard

Open the New Organization wizard to start the process of creating an organization.

Procedure

1 Click the Manage & Monitor tab and then click Organizations in the left pane.

2 Click the New Organization button.

   The New Organization wizard starts.

Name the Organization

Provide a descriptive name and an optional description for your new organization.

Procedure

1 Type an organization name.

   This name provides a unique identifier that appears as part of the URL that members of the organization use to log in to the organization.

2 Type a display name for the organization.

   This name appears in the browser header when an organization member uses the unique URL to log in to vCloud Director. An administrator or organization administrator can change this name later.

3 (Optional) Type a description of the organization.

4 Click Next.

Specify the Organization LDAP Options

You can use an LDAP service to provide a directory of users and groups for the organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. Only a system administrator can set LDAP options. An organization administrator cannot modify LDAP options.

For more information about entering custom LDAP settings, see Configuring System LDAP Settings.

Procedure

1 Select the source for organization users.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Organization administrator creates a local user account for each user in the organization. You cannot create groups if you select this option.</td>
</tr>
<tr>
<td>VCD system LDAP service</td>
<td>Use the vCloud Director system LDAP service as the source for organization users and groups.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Connect the organization to its own private LDAP service.</td>
</tr>
</tbody>
</table>
2 Provide any additional information that your selection requires.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Click Next.</td>
</tr>
<tr>
<td>VCD system LDAP service</td>
<td>(Optional) Type the distinguished name of the organizational unit (OU) to use to limit the users that you can import into the organization and click Next. If you do not enter anything, you can import all users in the system LDAP service into the organization. <strong>Note</strong> Specifying an OU does not limit the LDAP groups you can import. You can import any LDAP group from the system LDAP root. However, only users who are in both the OU and the imported group can log in to the organization.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Click Next and enter the custom LDAP settings for the organization.</td>
</tr>
</tbody>
</table>

Add Local Users to the Organization

Every organization should have at least one local organization administrator account, so that users can log in even if the LDAP and SAML services are unavailable.

Procedure

1 Click **Add**.
2 Type a user name and password.
3 Assign a role to the user.
4 (Optional) Type the contact information for the user.
5 Select **Unlimited** or type a user quota for stored and running virtual machines and click **OK**. These quotas limit the user’s ability to consume storage and compute resources in the organization. If you set a quota here that is different from the quota set at the organization level, this quota takes precedence.
6 Click **Next**.

Set the Organization Catalog Sharing, Publishing, and Subscription Policies

Catalogs provide organization users with catalogs of vApp templates and media that they can use to create vApps and install applications on virtual machines.

Catalogs can be shared between organizations in different instances of vCloud Director, between organizations in the same instance of vCloud Director, or remain accessible only within the host organization.
Procedure

1 Set the organization catalog policies.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow sharing catalogs to other organizations</td>
<td>Allows organization administrators to share this organization's catalogs with other organizations in this instance of vCloud Director. If you do not select this option, organization administrators are still able to share catalogs within the organization.</td>
</tr>
<tr>
<td>Allow creation of catalog feeds for consumption by external organizations</td>
<td>Allows organization administrators to share this organization's catalogs with organizations outside this instance of vCloud Director.</td>
</tr>
<tr>
<td>Allow subscription to external catalog feeds</td>
<td>Allows organization administrators to subscribe this organization to catalog feeds from outside this instance of vCloud Director.</td>
</tr>
</tbody>
</table>

2 Click Next.

Configure Email Preferences

vCloud Director requires an SMTP server to send user notification and system alert emails. An organization can use the system email settings or use its own email settings.

Procedure

1 Select an SMTP server option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default SMTP server</td>
<td>The organization uses the system SMTP server.</td>
</tr>
<tr>
<td>Set organization SMTP server</td>
<td>The organization uses its own SMTP server. Type the DNS host name or IP address and port number of the SMTP server. (Optional) Select the Requires authentication check box and type a user name and password.</td>
</tr>
</tbody>
</table>

2 Select a notification settings option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default notification settings</td>
<td>The organization uses the system notification settings.</td>
</tr>
<tr>
<td>Set organization notification settings</td>
<td>The organization uses its own notification settings. Type an email address that appears as the sender for organization emails, type text to use as the subject prefix for organization emails, and select the recipients for organization emails.</td>
</tr>
</tbody>
</table>

3 (Optional) Type a destination email address and click Test Email Settings to verify that all SMTP server settings are configured as expected.

4 Click Next.

Configure Organization Lease, Quota, and Limit Settings

Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. Use these settings to prevent users from depleting or monopolizing an organization's resources.
For more information about leases, see Understanding Leases.

**Procedure**

1. Select the lease options for vApps and vApp templates.
   
   Leases provide a level of control over an organization’s storage and compute resources by specifying the maximum amount of time that vApps can run and that vApps and vApp templates can be stored. You can also specify what happens to vApps and vApp templates when their storage lease expires.

2. Select the quotas for running and stored virtual machines.
   
   Quotas determine how many virtual machines each user in the organization can store and power on in the organization’s virtual datacenters. The quotas that you specify act as the default for all new users added to the organization. Quotas set at the user level take precedence over quotas set at the organization level.

3. Select the limits for resource intensive operations.
   
   Certain vCloud Director operations, for example copy and move, are more resource intensive than others. Limits prevent resource intensive operations from affecting all the users in an organization and also provide a defense against denial-of-service attacks.

4. Select the number of simultaneous VMware Remote Console connections for each virtual machine.
   
   You might want to limit the number of simultaneous connections for performance or security reasons.

   **Note** This setting does not affect Virtual Network Computing (VNC) or Remote Desktop Protocol (RDP) connections.

5. (Optional) Select the **Account lockout enabled** check box, select the number of invalid logins to accept before locking a user account, and select the lockout interval.

6. Click **Next**.

**Confirm Settings and Create the Organization**

Before you create the organization, review the settings you entered.

**Procedure**

1. Review the settings for the organization.

2. (Optional) Click **Back** to modify the settings.

3. Click **Finish** to accept the settings and create the organization.

**What to do next**

Allocate resources to the organization.
Allocate Resources to an Organization

You allocate resources to an organization by creating an organization virtual datacenter that is partitioned from a provider virtual datacenter. A single organization can have multiple organization virtual datacenters.

Prerequisites

You must have a provider virtual datacenter before you can allocate resources to an organization.

Procedure

1. Open the Allocate Resources Wizard
   Open the Allocate Resources wizard to start the process of creating an organization virtual datacenter for an organization.

2. Select a Provider Virtual Datacenter
   An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

3. Select an Allocation Model
   The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

4. Configure the Allocation Model
   Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

5. Allocate Storage
   An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual datacenter datastores.

6. Network Pool and Services
   A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks.

7. Configure an Edge Gateway
   You configure an edge gateway to provide connectivity to one or more external networks.

8. Configure External Networks
   Select the external networks that the edge gateway can connect to.

9. Configure IP Settings on a New Edge Gateway
   Configure IP settings for external networks on the new edge gateway.

10. Suballocate IP Pools on a New Edge Gateway
    Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.
11 Configure Rate Limits on a New Edge Gateway
Configure the inbound and outbound rate limits for each external network on the edge gateway.

12 Create an Organization Virtual Datacenter Network
You can create an organization virtual datacenter network that is connected to the new edge gateway.

13 Name the Organization Virtual Datacenter
You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization virtual datacenter.

14 Confirm Settings and Create the Organization Virtual Datacenter
Before you create the organization virtual datacenter, review the settings you entered.

What to do next
Add a network to the organization.

Open the Allocate Resources Wizard
Open the Allocate Resources wizard to start the process of creating an organization virtual datacenter for an organization.

Procedure
1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Allocate Resources from the menu.
   The Allocate Resources wizard starts.

Select a Provider Virtual Datacenter
An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

Procedure
1. Select a provider virtual datacenter.
   The provider virtual datacenter list displays information about available resources and the networks list displays information about networks available to the selected provider virtual datacenter.
2. Click Next.

Select an Allocation Model
The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.
Prerequisites

Verify that you understand which allocation model is appropriate for your environment. See Understanding Allocation Models.

Procedure

1. Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>A percentage of the resources you allocate from the provider virtual datacenter are committed to the organization virtual datacenter. You can specify the percentage for both CPU and memory.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are committed only when users create vApps in the organization virtual datacenter.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

For information about the placement engine and virtual machine shares, rates and limits, see the vCloud Director User's Guide.

2. Click Next.

Configure the Allocation Model

Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

Procedure

1. Select the allocation model options.

   Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default value for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the CPU allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization virtual datacenter are assigned this amount of GHz per vCPU. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the memory allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

2 **Click Next.**

**Example: Configuring an Allocation Model**

When you create an organization virtual datacenter, vCloud Director creates a vSphere resource pool based on the allocation model settings you specify.

**Table 3-1. How Allocation Pool Settings Affect Resource Pool Settings When Single Cluster Allocation Pool is Enabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>25GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>50GB</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>10GB</td>
</tr>
</tbody>
</table>

**Table 3-2. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>Sum of the number of vCPU times vCPU frequency for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>Sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>2.5GHz</td>
</tr>
</tbody>
</table>
Table 3-2. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled (Continued)

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Limit</td>
<td>Sum of the configured memory size for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>Sum of the configured memory size times the percentage guarantee for memory for all associated virtual machines</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Table 3-3. How Pay-As-You Go Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation, CPU Limit</td>
<td>0.00GHz, Unlimited</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>100%</td>
<td>Memory Reservation, Memory Limit</td>
<td>0.00GB, Unlimited</td>
</tr>
</tbody>
</table>

Resource pools created to support Pay-As-You-Go organization virtual datacenters never have reservations or limits. Pay-As-You-Go settings affect only overcommitment. A 100 percent guarantee means overcommitment is impossible. The lower the percentage, the more overcommitment is possible.

Table 3-4. How Reservation Pool Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th>Reservation Pool Setting</th>
<th>Reservation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Allocate Storage

An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual datacenter datastores.

Thin provisioning can help you avoid over-allocating storage. For a virtual machine with a thin-provisioned virtual disk, ESXi reserves all the storage dictated by disk’s maximum capacity, but commits only as much storage as the disk needs for its initial operations. Additional storage is committed as the disk requires it.

Fast provisioning saves time by using linked clones where possible. See Fast Provisioning of Virtual Machines.

Procedure

1. Select the storage policy to allocate and click Add.
2. Enter the amount of storage to allocate.
3 Select a **Default instantiation policy** from the drop-down menu.

This is the default storage policy used for all virtual machine provisioning operations where the storage policy is not specified at the virtual machine or vApp template level.

4 (Optional) Select the **Enable thin provisioning** check box to enable thin provisioning for virtual machines in the organization virtual datacenter.

5 (Optional) Deselect the **Enable fast provisioning** check box to disable fast provisioning for virtual machines in the organization virtual datacenter.

6 Click **Next**.

**Network Pool and Services**

A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks.

**Procedure**

1 Select a network pool or select **None**.

   If you select **None**, you can add a network pool later.

2 (Optional) Convert the selected network pool to a VXLAN pool.

   If the selected network pool is a VCDNI pool, a **Migrate to VXLAN** button is displayed. See VMware Knowledge Base article [https://kb.vmware.com/kb/2148381](https://kb.vmware.com/kb/2148381).

3 Enter the maximum number of networks that the organization can provision from the network pool.

4 (Optional) Select **Enable** for each available third-party or edge gateway service to enable.

5 Click **Next**.

**Configure an Edge Gateway**

You configure an edge gateway to provide connectivity to one or more external networks.

**Procedure**

1 Select an edge gateway configuration based on your system resources.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>Requires less memory and compute resources.</td>
</tr>
<tr>
<td>Large</td>
<td>Provides increased capacity and performance than with the Compact option.</td>
</tr>
<tr>
<td></td>
<td>Large and X-Large configurations provide identical security functions.</td>
</tr>
<tr>
<td>X-Large</td>
<td>Suited for environments that have a load balancer with large numbers of</td>
</tr>
<tr>
<td></td>
<td>concurrent sessions.</td>
</tr>
<tr>
<td>Quad Large</td>
<td>Recommended for high throughput and requires a high connection rate.</td>
</tr>
</tbody>
</table>

For more information on system requirements for deploying an edge gateway, see *System Requirements for NSX* in the *NSX Administration Guide*. 
2 (Optional) Select **Enable High Availability** to enable automatic failover to a backup edge gateway.

3 (Optional) Select **Create as Advanced Gateway** to enable use of the vCloud Director Tenant Portal to configure NSX services on the gateway.

   **Important** Existing vCloud API clients might not be able to complete some operations on an advanced Edge Gateway. See [http://kb.vmware.com/kb/2147625.](http://kb.vmware.com/kb/2147625)

4 (Optional) Select **Enable Distributed Routing** to configure an advanced gateway to provide distributed logical routing.

   This option is available only if you select **Create as Advanced Gateway**. When you enable Distributed Routing, you can create many more organization VDC networks on the gateway. Traffic on those networks is optimized for VM-to-VM communication.

5 (Optional) Select **Configure IP Settings** to manually configure the external interface’s IP address.

6 (Optional) Select **Sub-Allocate IP Pools** to allocate a set of IP addresses for gateway services to use.

7 (Optional) Select **Configure Rate Limits** to choose the inbound and outbound rate limits for each externally connected interface.

8 Click **Next**.

### Configure External Networks

Select the external networks that the edge gateway can connect to.

This page appears only if you selected **Create a new edge gateway**.

**Procedure**

1 Select an external network from the list and click **Add**.

   Hold down Ctrl to select multiple networks.

2 Select a network to be the default gateway.

3 (Optional) Select **Use default gateway for DNS Relay**.

4 Click **Next**.

### Configure IP Settings on a New Edge Gateway

Configure IP settings for external networks on the new edge gateway.

This page appears only if you selected **Configure IP Settings** during gateway configuration.

**Procedure**

1 On the **Configure IP Settings** page, click **Change IP Assignment**.

2 Select **Manual** from the drop-down menu for each external network for which to specify an IP address.
3 Type an IP address for each external network set to Manual and click Next.

**Suballocate IP Pools on a New Edge Gateway**

Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.

This page appears only if you selected **Sub-Allocate IP Pools** during gateway configuration.

**Procedure**

1 Select an external network and IP pool to suballocate.
2 Type an IP address or range of IP addresses within the IP pool range and click Add.
   Repeat this step to add multiple suballocated IP pools.
3 (Optional) Select a suballocated IP pool and click Modify to modify the IP address range of the suballocated IP pool.
4 (Optional) Select a suballocated IP pool and click Remove to remove the suballocated IP pool.
5 Click Next.

**Configure Rate Limits on a New Edge Gateway**

Configure the inbound and outbound rate limits for each external network on the edge gateway.

This page appears only if you selected **Configure Rate Limits** during gateway configuration. Rate limits apply only to external networks backed by distributed port groups with static binding.

**Procedure**

1 Click Enable for each external network on which to enable rate limits.
2 Type the Incoming Rate Limit in gigabits per second for each enabled external network.
3 Type the Outgoing Rate Limit in gigabits per second for each enabled external network and click Next.

**Create an Organization Virtual Datacenter Network**

You can create an organization virtual datacenter network that is connected to the new edge gateway.

This page appears only if you selected **Create a new edge gateway**.

**Procedure**

1 (Optional) Select Create a network for this virtual datacenter connected to this new edge gateway.
2 Type a name and optional description for the new organization virtual datacenter network.
3 (Optional) Select Share this network with other VDCs in the organization.
4 Type a gateway address and network mask for the organization virtual datacenter network.
5 (Optional) Select **Use gateway DNS** to use the DNS relay of gateway.
   This option is available only if the gateway has DNS relay enabled.

6 (Optional) Enter DNS settings to use DNS.

7 Enter an IP address or range of IP addresses and click **Add** to create a static IP pool.
   Repeat this step to add multiple static IP pools.

8 Click **Next**.

### Name the Organization Virtual Datacenter

You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization virtual datacenter.

**Procedure**

1. Type a name and optional description.
   
   Avoid using special characters in the name and description fields. Length limitations are documented in [Length Limits on Names and Descriptions](#).

2. (Optional) Deselect **Enabled**.
   Disabling the organization virtual datacenter prevents new vApps from being deployed to the virtual datacenter. Running vApps continue to run but additional vApps cannot be started.

3 Click **Next**.

### Confirm Settings and Create the Organization Virtual Datacenter

Before you create the organization virtual datacenter, review the settings you entered.

**Procedure**

1 Review the settings for the organization virtual datacenter.

2 (Optional) Click **Back** to modify the settings.

3 (Optional) Select **Add networks to this organization after this wizard is finished** to immediately create an organization virtual datacenter network for this virtual datacenter.

4 Click **Finish** to accept the settings and create the organization virtual datacenter.
   
   When you create an organization virtual datacenter, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.
A newly created organization has no catalogs in it. After an organization administrator or catalog author creates a catalog, members of the organization can use it as a destination for uploads or a source of subscription-based content.

Organizations use catalogs to store vApp templates and media files. Organization members use catalog items as the building blocks to create their own vApps.

Catalog Contents

Catalogs contain references to vApp templates and media images. You can configure a catalog in several different ways:

- as a repository for local content that can remain private to the catalog owner or can be shared with other users, groups, or organizations in your cloud
- as a source of published content, to which other clouds can subscribe.
- as a local repository for content published by another cloud or any Web site that hosts a VMware Content Subscription Protocol (VCSP) endpoint.

An organization administrator or catalog owner controls catalog sharing. Organization administrators in organizations that have permission to publish catalogs control publication and subscription options for catalogs in their organization. A system administrator can enable background synchronization of catalogs with external sources and set background synchronization schedules to regulate consumption of network bandwidth by this activity.

Access to Catalogs

A catalog initially grants full control to its owner and no access to other users. The catalog owner, an organization administrator, or a catalog author can grant catalog access to other members of the organization, individually or collectively. Organization administrators and system administrators can share a catalog with other organizations in the cloud.

This chapter includes the following topics:

- Add a New Catalog
- Access a Catalog
- Share A Catalog
- Publish a Catalog to an External Organization
- Change the Owner of a Catalog
- Delete a Catalog
- Change the Properties of a Catalog
- Subscribe to an External Catalog Feed

Add a New Catalog

You can create catalogs to group your vApp templates and media files.

Prerequisites

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

Procedure

1. Click Catalogs and select My Organization's Catalogs in the left pane.
2. On the Catalogs tab, click Add Catalog.
3. Type a catalog name and optional description and click Next.
4. Select the type of storage to use for vApp templates and ISOs in this catalog and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use any available storage in the organization</td>
<td>This catalog uses any available storage in the organization.</td>
</tr>
<tr>
<td>Pre-provision storage on specific storage policy</td>
<td>Select a virtual datacenter storage policy to use for this catalog’s vApp templates and ISOs and click Add. The selected storage policy causes the vApp template size to count against your catalog storage quota.</td>
</tr>
</tbody>
</table>
5 Click **Add Members**.

**Note**  This option might be unavailable, depending on your organizational settings.

a Select which users and groups in the organization can access this catalog.
   - Select **Everyone in this organization** to grant catalog access to all users and groups in the organization.
   - Select **Specific users and groups** to grant catalog access to certain users or groups and click **Add**.

b Select the access level for users with access to this catalog from the drop-down menu and click **OK**.
   - Select **Read Only** to grant read access to the catalog’s vApp templates and ISOs.
   - Select **Read/Write** to grant read access to the catalog’s vApp templates and ISOs, and to allow user to add vApp templates and ISOs to the catalog.
   - Select **Full Control** to grant full access to the catalog’s contents and settings.

6 Click **Add Organizations**.

**Note**  This option might be unavailable, depending on your organizational settings.

a Select which organizations on this vCloud Director installation can access this catalog.
   - Select **All organizations** to grant catalog access to all organizations in the vCloud Director installation.
   - Select **Specific organizations** to grant catalog access to certain organizations and click **Add**.

b Select the access level for users with access to this catalog from the drop-down menu and click **OK**.
   - Select **Read Only** to grant read access to the catalog's vApp templates and ISOs.
   - Select **Read/Write** to grant read access to the catalog's vApp templates and ISOs, and to allow organizations to add vApp templates and ISOs to the catalog.
   - Select **Full Control** to grant full access to the catalog's contents and settings.

7 Click **Next**.

8 (Optional) Select **Enabled** and click to allow the creation of a catalog feed for consumption by catalogs outside this vCloud Director installation and supply a password for the catalog feed.

9 (Optional) Select **Enable early catalog export to optimize synchronization**.

   Before selecting this option, verify that you have available storage at the transfer server location for the exported catalog.
10  (Optional) Select **Preserve identity information** to include BIOS and UUID information in the downloaded OVF package.

    Enabling this option limits portability of the OVF package.

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

The new catalog appears in My Organization's Catalogs. A catalog's displayed status on this page does not reflect the status of the templates and vApps in the catalog.

**Access a Catalog**

You can access catalogs in your organization if they have been shared with you. You can access public catalogs if an organization administrator has made them accessible in your organization.

**Prerequisites**

Catalog access is controlled by catalog sharing, not by the rights in your role.

**Procedure**

1  Click **Catalogs**.

2  In the left pane, click a catalog option.

3  In the right pane, select a catalog, right-click, and select **Open**.

**Share A Catalog**

You can share a catalog with all members of your organization, or with specific members. You can also publish it to external organizations.

**Prerequisites**

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

**Procedure**

1  Click **Catalog** and select **My Organization's Catalogs** in the left pane.

2  On the **Catalogs** tab, right-click the catalog name and select **Publish Settings**.

3  On the **Sharing** tab, click **Add Members**.

4  Select which users and groups in the organization can access this catalog.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Everyone in this organization</strong></td>
<td>All users and groups in the organization have access to this catalog.</td>
</tr>
<tr>
<td><strong>Specific users and groups</strong></td>
<td>Select users or groups to grant catalog access to and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
Select the access level for users with access to this catalog from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only</td>
<td>Users with access to this catalog have read access to the catalog's vApp templates and ISOs.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Users with access to this catalog have read access to the catalog's vApp templates and ISOs and can add vApp templates and ISOs to the catalog.</td>
</tr>
<tr>
<td>Full Control</td>
<td>Users with access to this catalog have full control of the catalog's contents and settings.</td>
</tr>
</tbody>
</table>

(Optional) Click **External Publishing** to specify external publishing options.

This option is available only if the system administrator has granted your organization permission to publish externally.

a Select **Enable Publishing** to publish this catalog to all organizations in the system.

You can optionally require organization administrators to use a password when enabling access to this catalog in their organizations.

b Select **Preserve Identity Information** to include BIOS UUIDs and MAC addresses in published vApp templates.

Identity information might not be usable in all other organizations.

Click **OK** to save your changes.

**Publish a Catalog to an External Organization**

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

**Prerequisites**

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

**Procedure**

1. Click **Catalog** and select **My Organization's Catalogs** in the left pane.
2. On the **Catalogs** tab, right-click the catalog name and select **Publish Settings**.
3. On the **External Publishing** tab, select **Enabled** and supply a password for the catalog feed.
4. Click **OK**.

**What to do next**

Provide the subscription URL listed on the **External Publishing** tab and the password to grant access to the catalog. An organization must subscribe to the catalog to gain access to its contents.
Change the Owner of a Catalog

An administrator can change the owner of a catalog.

Before you can delete a user who owns a catalog, you must change the owner or delete the catalog.

Prerequisites

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

Procedure

1. Select Catalog > My Organization's Catalogs.
2. Click the Catalogs tab, right-click a catalog, and select Change Owner.
3. Select a user from the list or search for one.
   You can search for a user by full name or by user name.
4. Click OK.

Delete a Catalog

You can delete a catalog from your organization.

Prerequisites

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

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

Procedure

1. Click Catalog.
2. In the left pane, click My Organization's Catalogs.
3. Select a catalog, right-click, and select Delete.
4. Click Yes to confirm.

The empty catalog is deleted from your organization.

Change the Properties of a Catalog

You can review and change catalog properties.
Prerequisites
This operation requires the rights included in the predefined Catalog Author role or an equivalent set of rights.

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

You must be the owner of the catalog.

Procedure
1. Click Catalog.
2. In the left pane, click My Organization's Catalogs.
3. Select a catalog, right-click, and select Properties.
4. Review the properties in the General, Sharing, and External Publishing tabs.
5. Change the relevant properties and click OK.

Your catalog properties are updated.

Subscribe to an External Catalog Feed
You subscribe to an external catalog feed to allow your organization access to a catalog from an outside source.

An external catalog is one provided by a source that is not an organization in the same vCloud Director installation as your organization.

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

Procedure
1. Click Catalogs and select My Organization's Catalogs in the left pane.
2. Click Add Catalog and type a name and optional description for the catalog feed.
3. Select Subscribe to an external catalog and click Next.
4. Select the type of storage to use for this catalog feed and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use any available storage in the organization</td>
<td>This catalog feed uses any available storage in the organization.</td>
</tr>
<tr>
<td>Pre-provision storage on specific storage policy</td>
<td>Select a virtual datacenter storage policy to use for this catalog feed and click Add.</td>
</tr>
</tbody>
</table>
5 Click **Add Members**.

6 Select which users and groups in the organization can access this catalog feed and click **OK**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone in this organization</td>
<td>All users and groups in the organization have access to this catalog feed.</td>
</tr>
<tr>
<td>Specific users and groups</td>
<td>Select users or groups to which to grant catalog feed access and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

7 Click **Add Organizations**.

8 Select which organizations on this vCloud Director installation can access this catalog feed and click **OK**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All organizations</td>
<td>All organizations in the vCloud Director installation have access to this catalog feed.</td>
</tr>
<tr>
<td>Specific organizations</td>
<td>Select the organizations to which to grant catalog feed access and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

9 Click **Next**.

10 Review the catalog feed settings and click **Finish**.
Managing Cloud Resources

Provider virtual datacenters, organization virtual datacenters, external networks, organization virtual datacenter networks, and network pools are all considered cloud resources. After you add cloud resources to vCloud Director, you can modify them and view information about their relationships with each other.

This chapter includes the following topics:

- Managing Provider Virtual Datacenters
- Managing Organization Virtual Datacenters
- Managing Organization Virtual Data Center Templates
- Managing External Networks
- Managing Edge Gateways
- Managing Organization Virtual Datacenter Networks
- Managing Network Pools
- Managing Cloud Cells
- Managing Service Offerings
- Configuring and Managing Multisite Deployments
- Create or Update Object Metadata

Managing Provider Virtual Datacenters

After you create a provider virtual datacenter, you can modify its properties, disable or delete it, and manage its ESXi hosts and datastores.

Enable or Disable a Provider Virtual Datacenter

You can disable a provider virtual datacenter to prevent the creation of organization virtual datacenters that use the provider virtual datacenter resources.

When you disable a provider virtual datacenter, vCloud Director also disables the organization virtual datacenters that use its resources. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.
Procedure
1. Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.
2. Right-click the provider virtual datacenter name and select **Enable** or **Disable**.

### Delete a Provider Virtual Datacenter
You can delete a provider virtual datacenter to remove its compute, memory, and storage resources from vCloud Director. The resources remain unaffected in vSphere.

**Prerequisites**
- Disable the provider virtual datacenter.
- Disable and delete all organization virtual datacenters that use the provider virtual datacenter.

**Procedure**
1. Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.
2. Right-click the provider virtual datacenter name and select **Delete**.
3. Click **Yes**.

### Modify a Provider Virtual Datacenter Name and Description
As your vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing provider virtual datacenter.

**Procedure**
1. Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.
2. Right-click the provider virtual datacenter name and select **Properties**.
3. Type a new name or description and click **OK**.
   - You can use the name and description fields to indicate the vSphere functionality available to the provider virtual datacenter, for example, vSphere HA.

### Merge Provider Virtual Datacenters
You can merge two or more provider virtual datacenters into a single provider virtual datacenter, combining the resources of all merged provider virtual datacenters.

**Procedure**
1. Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.
2. Right-click the provider virtual datacenter to merge other provider virtual datacenters to and select **Merge with**.
3. Select one or more provider virtual datacenters to merge with this one and click **Add**.
   - Hold down Ctrl to select multiple provider virtual datacenters.
(Optional) Enter a new name and description for the provider virtual datacenter.

Click OK.

The selected provider virtual datacenters are merged into this provider virtual datacenter.

Manage Provider Virtual Datacenter Hosts

You can disable a host to prevent vApps from starting up on the host. Virtual machines that are already running on the host are not affected.

For additional ESXi host management options, see Managing vSphere ESXi Hosts.

Procedure

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Hosts tab.
4. Right-click the host name and select Enable Host or Disable Host.

Enable VXLAN on a Legacy Provider VDC

vSphere VXLAN is enabled by default for new provider VDCs. A system administrator must manually enable VXLAN on a Provider VDC that was created with an older release of vCloud Director.

Prerequisites

This operation is restricted to system administrators.

Configure VXLAN for your vCloud Director environment. See the NSX Administration Guide.

Procedure

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the Provider VDC name and select Enable VXLAN.

A VXLAN network pool is created for the Provider VDC. See VXLAN Network Pools.

Provider Virtual Datacenter Datastores

Provider virtual datacenter datastores provide storage capacity for provider virtual datacenters.

Provider Virtual Datacenter Datastore Metrics

The following information about each provider virtual datacenter datastore appears on the Datastores tab of a provider virtual datacenter.
### Table 5-1. Datastore Metrics

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the provider virtual datacenter datastore.</td>
</tr>
<tr>
<td>Enabled</td>
<td>A checkmark appears when the provider virtual datacenter datastore is enabled.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of file system the datastore uses, either Virtual Machine File System (VMFS) or Network File System (NFS).</td>
</tr>
<tr>
<td>Used</td>
<td>The datastore space occupied by virtual machine files, including log files, snapshots, and virtual disks. When a virtual machine is powered on, the used storage space also includes log files.</td>
</tr>
<tr>
<td>Provisioned</td>
<td>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.</td>
</tr>
<tr>
<td>Requested</td>
<td>Provisioned storage in use only by vCloud Director-managed objects on the datastore. If thin provisioning is enabled on vCloud Director, some of the requested space might not be in use.</td>
</tr>
<tr>
<td>vCenter</td>
<td>The vCenter Server associated with the datastore.</td>
</tr>
</tbody>
</table>

### Add a VM Storage Policy to a Provider Virtual Data Center

Add a VM storage policy to a provider virtual data center so that the storage policy supports the organization virtual data centers backed by the provider virtual data center.

VM storage policies are created and managed in vSphere. For information about Storage Policy Based Management (SPBM), see the vSphere Storage documentation or contact your vSphere administrator.

**Important** vCloud Director does not support VM storage policies for host-based data services such as encryption and storage I/O control.

**Prerequisites**

Log in to the vCloud Director Web Console as a **system administrator**.

**Procedure**

1. On the **Manage & Monitor** tab, in the left pane, click **Provider VDCs**.
2. Right-click the provider virtual data center name and click **Open**.
3. On the **Storage Policies** tab, click **Add Storage Policy**.
4. Select a storage policy and click **Add**.
   - If you select **Any**, vCloud Director dynamically adds and removes datastores as they are added to or removed from the datastore clusters of the provider virtual data center.
5. Click **OK**.
Support for the storage policy is added to 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 Storage Policy to an Organization Virtual Datacenter](#).

## Configure Storage I/O Control Support in a Provider VDC

If you want to enable specification of hard disk read/write performance by members of an organization, a Provider VDC that supports the organization must include a storage profile that is backed by an appropriately configured vSphere datastore.

Managed read/write performance in physical storage devices and virtual disks is defined in units called IOPS, which measure read/write operations per second. When an organization VDC storage profile is backed by a Provider VDC storage profile that includes storage devices that are capable of IOPS allocation, you 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, even 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 profile whose maximum IOPS value is lower than the requested value, or a storage profile that is not configured with IOPS support.

When backed by an appropriately configured Provider VDC storage profile, storage profiles in an organization VDC can be configured to support delivery of a specified level of I/O performance to disks that use them. See the [vCloud API Programming Guide for Service Providers](#) for information about configuring storage I/O control support in an organization VDC.

### Prerequisites

This operation is restricted to system administrators.

### Procedure

1. Choose or create an appropriately configured vSphere storage policy.

   Before vCloud Director can enable IOPS for a Provider VDC storage profile, an IOPS-enabled vSphere storage policy must exist on a vCenter server registered to vCloud Director.

   - The storage devices backing the underlying vSphere datastores must be capable of IOPS support.

   **Note** You cannot enable IOPS support on a VMware Virtual SAN datastore.

   - A vSphere administrator must configure the datastores with a specific vSphere custom field and value, as described in VMware Knowledge Base article [http://kb.vmware.com/kb/2148300](http://kb.vmware.com/kb/2148300)

   - A vSphere administrator must create a vSphere storage policy that includes the IOPS-capable datastore.
2 Include the IOPS-capable vSphere storage profile in a Provider VDC.

Reference the IOPS-capable vSphere storage profile by name in a ProviderVdcStorageProfile element in the VMwProviderVdcParams request body you use when creating a Provider VDC or in the UpdateProviderVdcStorageProfiles element in an updateStorageProfiles request body you use when updating Provider VDC storage profiles.

**Edit the Metadata for a Storage Policy on a Provider Virtual Datacenter**

You can edit the metadata for a storage policy on a provider virtual datacenter.

**Procedure**

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Storage Policies tab.
4. Right-click a storage policy and select Properties.
5. Edit the metadata as appropriate and click OK.

**Add a Resource Pool to a Provider VDC**

You can add additional resource pools to a provider VDC so that Pay-As-You-Go and Allocation Pool organization virtual datacenters that the provider virtual datacenter provides can expand.

When compute resources are backed by multiple resource pools, they can expand as needed to accommodate more virtual machines.

**Note** You can create resource pools backed by vSphere clusters that are optimally configured for hosting NSX edges that have VLAN uplinks, then use vCloud Director metadata to indicate that the system should 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**

This operation is restricted to system administrators.

Verify that additional more resource pools are available in the vCenter that supplies provider VDC’s primary resource pool.

**Procedure**

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Resource Pools tab.
vCloud Director adds a resource pool for the provider virtual datacenter to use, making elastic all Pay-As-You-Go and Allocation Pool organization virtual datacenters backed by the provider virtual datacenter.

vCloud 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. Do not edit or delete the system virtual datacenter resource pool.

**Enable or Disable a Provider Virtual Datacenter Resource Pool**

When you disable a resource pool, the memory and compute resources of the resource pool are no longer available to the provider virtual datacenter.

You must have at least one enabled resource pool on a provider virtual datacenter. Disabling a resource pool does not prevent its resources from being used by processes that are already in progress.

**Procedure**

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Resource Pools tab.
4. Right-click the resource pool and click Enable or Disable.

**Detach a Resource Pool From a Provider Virtual Datacenter**

If a provider virtual datacenter has more than one resource pool, you can detach a resource pool from the provider virtual datacenter.

**Prerequisites**

1. Disable the resource pool on the provider virtual datacenter.
2. Migrate any virtual machines from that resource pool to an enabled resource pool.
3. Redeploy any networks that are affected by the disabled resource pool.
4. Redeploy any edge gateways that are affected by the disabled resource pool.

**Procedure**

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Resource Pools tab.
4. Right-click the resource pool and click Detach.
Migrate Virtual Machines Between Resource Pools on a Provider Virtual Datacenter

You can migrate virtual machines from one resource pool to another on the same provider virtual datacenter. 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 provider virtual datacenter's resources.

Virtual machines that are part of a reservation pool organization virtual datacenter cannot be migrated. Templates and media should be migrated separately using datastore migration.

Prerequisites

Verify that you have at least one resource pool on the provider virtual datacenter other than the resource pool the virtual machines are on.

Procedure

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3. Click the Resource Pools tab.
4. Right-click the resource pool name and select Open.
5. Right-click the virtual machine name and select Migrate to.
   Hold down Ctrl and click to select multiple virtual machines.
6. Choose how to select the destination resource pool for the virtual machine.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically select a resource pool</td>
<td>vCloud Director chooses the destination resource pool for the virtual machines based on the current resource balance of all available resource pools.</td>
</tr>
<tr>
<td>Manually select a resource pool</td>
<td>Select a resource pool from the list of available resource pools to which to migrate the virtual machines to.</td>
</tr>
</tbody>
</table>
7. Click OK.

Configure Low Disk Space Thresholds for a Provider Virtual Datacenter Datastore

You can configure low disk space thresholds on a datastore to receive an email from vCloud 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.

Procedure

1. Click the Manage & Monitor tab and click Provider VDCs in the left pane.
2. Right-click the provider virtual datacenter name and select Open.
3 Click the **Datastores** tab.

4 Right-click the datastore name and select **Properties**.

5 Select the disk space thresholds for the datastore.

You can set two thresholds, yellow and red. When you set thresholds on a stand-alone datastore, they apply only to that datastore. If you set thresholds on a storage POD, they apply to all datastores in the storage POD. By default, vCloud Director sets the red threshold to 15% of the stand-alone datastore's or POD's total capacity and the yellow threshold to 25% of the stand-alone datastore or POD's total capacity.

When vCloud Director sends an email alert, the message indicates which threshold was crossed. When a datastore reaches its red threshold, the virtual machine placement engine stops placing virtual machines on the datastore.

Because the default thresholds on a storage POD are based on the total POD capacity, the thresholds might exceed the capacity of individual datastores within the POD. When setting thresholds on a storage POD, take into account the capacity of each datastore in the POD and set thresholds manually rather than accepting the default threshold configurations.

6 Click **OK**.

vCloud Director sets the thresholds for all provider virtual datacenters that use the datastore. vCloud Director sends an email alert when the datastore crosses the threshold.

**Send an Email Notification to Provider Virtual Datacenter Users**

You can send an email notification to all users who own objects in the provider virtual datacenter, for example, vApps or media files. You can send an email notification to let users know about upcoming system maintenance, for example.

**Prerequisites**

Verify that you have a valid connection to an SMTP server.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.

2 Right-click the provider virtual datacenter name and select **Notify**.

3 Type the email subject and message and click **Send Email**.

**Managing Organization Virtual Datacenters**

After you create an organization virtual datacenter, you can modify its properties, disable or delete it, and manage its allocation model, storage, and network settings.
Create an Organization Virtual Datacenter

Create an organization virtual datacenter to allocate resources to an organization. An organization virtual datacenter is partitioned from a provider virtual datacenter. A single organization can have multiple organization virtual datacenters.

Prerequisites

You must have a provider virtual datacenter before you can allocate resources to an organization.

Procedure

1. Open the New Organization Virtual Datacenter Wizard
   Open the New Organization virtual datacenter wizard to start the process of creating an organization virtual datacenter.

2. Select an Organization for the Organization Virtual Datacenter
   You can create an organization virtual datacenter to provide resources to any organization in the vCloud Director system. An organization can have more than one organization virtual datacenter.

3. Select a Provider Virtual Datacenter
   An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

4. Select an Allocation Model
   The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

5. Configure the Allocation Model
   Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

6. Allocate Storage
   An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual datacenter datastores.

7. Network Pool and Services
   A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks.

8. Configure an Edge Gateway
   You configure an edge gateway to provide connectivity to one or more external networks.

9. Configure External Networks
   Select the external networks that the edge gateway can connect to.

10. Configure IP Settings on a New Edge Gateway
    Configure IP settings for external networks on the new edge gateway.
11 Suballocate IP Pools on a New Edge Gateway
   Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.

12 Configure Rate Limits on a New Edge Gateway
   Configure the inbound and outbound rate limits for each external network on the edge gateway.

13 Create an Organization Virtual Datacenter Network
   You can create an organization virtual datacenter network that is connected to the new edge gateway.

14 Name the Organization Virtual Datacenter
   You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization virtual datacenter.

15 Confirm Settings and Create the Organization Virtual Datacenter
   Before you create the organization virtual datacenter, review the settings you entered.

Open the New Organization Virtual Datacenter Wizard

Open the New Organization virtual datacenter wizard to start the process of creating an organization virtual datacenter.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Click the add button.

Select an Organization for the Organization Virtual Datacenter

You can create an organization virtual datacenter to provide resources to any organization in the vCloud Director system. An organization can have more than one organization virtual datacenter.

Procedure
1. Select an organization.
2. Click Next.

Select a Provider Virtual Datacenter

An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

Procedure
1. Select a provider virtual datacenter.
   The provider virtual datacenter list displays information about available resources and the networks list displays information about networks available to the selected provider virtual datacenter.
2  Click **Next**.

**Select an Allocation Model**

The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

**Prerequisites**

Verify that you understand which allocation model is appropriate for your environment. See [Understanding Allocation Models](#).

**Procedure**

1  Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>A percentage of the resources you allocate from the provider virtual datacenter are committed to the organization virtual datacenter. You can specify the percentage for both CPU and memory.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are committed only when users create vApps in the organization virtual datacenter.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

For information about the placement engine and virtual machine shares, rates and limits, see the [vCloud Director User's Guide](#).

2  Click **Next**.

**Configure the Allocation Model**

Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

**Procedure**

1  Select the allocation model options.

Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default value for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the CPU allocation is committed for this organization virtual datacenter.</td>
</tr>
</tbody>
</table>
Option | Action
--- | ---
vCPU Speed | Enter the vCPU speed in GHz. Virtual machines running in the organization virtual datacenter are assigned this amount of GHz per vCPU. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.

Memory allocation | Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.

Memory resources guaranteed | Enter the percentage of memory resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the memory allocation is committed for this organization virtual datacenter.

Maximum number of VMs | Enter the maximum number of virtual machines that can be created in the organization virtual datacenter.

2 Click **Next**.

**Example: Configuring an Allocation Model**

When you create an organization virtual datacenter, vCloud Director creates a vSphere resource pool based on the allocation model settings you specify.

**Table 5-2. How Allocation Pool Settings Affect Resource Pool Settings When Single Cluster Allocation Pool is Enabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>25GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>50GB</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>10GB</td>
</tr>
</tbody>
</table>

**Table 5-3. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>Sum of the number of vCPU times vCPU frequency for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>Sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>2.5GHz</td>
</tr>
</tbody>
</table>
Table 5-3. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled (Continued)

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Limit</td>
<td>Sum of the configured memory size for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>Sum of the configured memory size times the percentage guarantee for memory for all associated virtual machines</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Table 5-4. How Pay-As-You-Go Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation, CPU Limit</td>
<td>0.00GHz, Unlimited</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>100%</td>
<td>Memory Reservation, Memory Limit</td>
<td>0.00GB, Unlimited</td>
</tr>
</tbody>
</table>

Resource pools created to support Pay-As-You-Go organization virtual datacenters never have reservations or limits. Pay-As-You-Go settings affect only overcommitment. A 100 percent guarantee means overcommitment is impossible. The lower the percentage, the more overcommitment is possible.

Table 5-5. How Reservation Pool Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th>Reservation Pool Setting</th>
<th>Reservation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Allocate Storage

An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual datacenter datastores.

Thin provisioning can help you avoid over-allocating storage. For a virtual machine with a thin-provisioned virtual disk, ESXi reserves all the storage dictated by disk's maximum capacity, but commits only as much storage as the disk needs for its initial operations. Additional storage is committed as the disk requires it.

Fast provisioning saves time by using linked clones where possible. See Fast Provisioning of Virtual Machines.

Procedure

1. Select the storage policy to allocate and click Add.
2. Enter the amount of storage to allocate.
3 Select a **Default instantiation policy** from the drop-down menu.

This is the default storage policy used for all virtual machine provisioning operations where the storage policy is not specified at the virtual machine or vApp template level.

4 (Optional) Select the **Enable thin provisioning** check box to enable thin provisioning for virtual machines in the organization virtual datacenter.

5 (Optional) Deselect the **Enable fast provisioning** check box to disable fast provisioning for virtual machines in the organization virtual datacenter.

6 Click **Next**.

**Network Pool and Services**

A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks.

**Procedure**

1 Select a network pool or select **None**.

   If you select **None**, you can add a network pool later.

2 (Optional) Convert the selected network pool to a VXLAN pool.

   If the selected network pool is a VCDNI pool, a **Migrate to VXLAN** button is displayed. See VMware Knowledge Base article [https://kb.vmware.com/kb/2148381](https://kb.vmware.com/kb/2148381).

3 Enter the maximum number of networks that the organization can provision from the network pool.

4 (Optional) Select **Enable** for each available third-party or edge gateway service to enable.

5 Click **Next**.

**Configure an Edge Gateway**

You configure an edge gateway to provide connectivity to one or more external networks.

**Procedure**

1 Select an edge gateway configuration based on your system resources.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>Requires less memory and compute resources.</td>
</tr>
<tr>
<td>Large</td>
<td>Provides increased capacity and performance than with the Compact option.</td>
</tr>
<tr>
<td>X-Large</td>
<td>Suited for environments that have a load balancer with large numbers of</td>
</tr>
<tr>
<td></td>
<td>concurrent sessions.</td>
</tr>
<tr>
<td>Quad Large</td>
<td>Recommended for high throughput and requires a high connection rate.</td>
</tr>
</tbody>
</table>

For more information on system requirements for deploying an edge gateway, see *System Requirements for NSX* in the *NSX Administration Guide*.

2 (Optional) Select **Enable High Availability** to enable automatic failover to a backup edge gateway.
3 (Optional) Select **Create as Advanced Gateway** to enable use of the vCloud Director Tenant Portal to configure NSX services on the gateway.

**Important** Existing vCloud API clients might not be able to complete some operations on an advanced Edge Gateway. See http://kb.vmware.com/kb/2147625.

4 (Optional) Select **Enable Distributed Routing** to configure an advanced gateway to provide distributed logical routing.

This option is available only if you select **Create as Advanced Gateway**. When you enable Distributed Routing, you can create many more organization VDC networks on the gateway. Traffic on those networks is optimized for VM-to-VM communication.

5 (Optional) Select **Configure IP Settings** to manually configure the external interface's IP address.

6 (Optional) Select **Sub-Allocate IP Pools** to allocate a set of IP addresses for gateway services to use.

7 (Optional) Select **Configure Rate Limits** to choose the inbound and outbound rate limits for each externally connected interface.

8 Click **Next**.

### Configure External Networks

Select the external networks that the edge gateway can connect to.

This page appears only if you selected **Create a new edge gateway**.

**Procedure**

1. Select an external network from the list and click **Add**.

   Hold down Ctrl to select multiple networks.

2. Select a network to be the default gateway.

3. (Optional) Select **Use default gateway for DNS Relay**.

4. Click **Next**.

### Configure IP Settings on a New Edge Gateway

Configure IP settings for external networks on the new edge gateway.

This page appears only if you selected **Configure IP Settings** during gateway configuration.

**Procedure**

1. On the **Configure IP Settings** page, click **Change IP Assignment**.

2. Select Manual from the drop-down menu for each external network for which to specify an IP address.

3. Type an IP address for each external network set to Manual and click **Next**.
Suballocate IP Pools on a New Edge Gateway

Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.

This page appears only if you selected **Sub-Allocate IP Pools** during gateway configuration.

**Procedure**

1. Select an external network and IP pool to suballocate.
2. Type an IP address or range of IP addresses within the IP pool range and click **Add**.
   
   Repeat this step to add multiple suballocated IP pools.
3. (Optional) Select a suballocated IP pool and click **Modify** to modify the IP address range of the suballocated IP pool.
4. (Optional) Select a suballocated IP pool and click **Remove** to remove the suballocated IP pool.
5. Click **Next**.

Configure Rate Limits on a New Edge Gateway

Configure the inbound and outbound rate limits for each external network on the edge gateway.

This page appears only if you selected **Configure Rate Limits** during gateway configuration. Rate limits apply only to external networks backed by distributed port groups with static binding.

**Procedure**

1. Click **Enable** for each external network on which to enable rate limits.
2. Type the **Incoming Rate Limit** in gigabits per second for each enabled external network.
3. Type the **Outgoing Rate Limit** in gigabits per second for each enabled external network and click **Next**.

Create an Organization Virtual Datacenter Network

You can create an organization virtual datacenter network that is connected to the new edge gateway.

This page appears only if you selected **Create a new edge gateway**.

**Procedure**

1. (Optional) Select **Create a network for this virtual datacenter connected to this new edge gateway**.
2. Type a name and optional description for the new organization virtual datacenter network.
3. (Optional) Select **Share this network with other VDCs in the organization**.
4. Type a gateway address and network mask for the organization virtual datacenter network.
5  (Optional) Select **Use gateway DNS** to use the DNS relay of gateway.  
   This option is available only if the gateway has DNS relay enabled.
6  (Optional) Enter DNS settings to use DNS.
7  Enter an IP address or range of IP addresses and click **Add** to create a static IP pool.  
   Repeat this step to add multiple static IP pools.
8  Click **Next**.

**Name the Organization Virtual Datacenter**

You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization virtual datacenter.

**Procedure**

1  Type a name and optional description.  
   Avoid using special characters in the name and description fields. Length limitations are documented in **Length Limits on Names and Descriptions**.
2  (Optional) Deselect **Enabled**.  
   Disabling the organization virtual datacenter prevents new vApps from being deployed to the virtual datacenter. Running vApps continue to run but additional vApps cannot be started.
3  Click **Next**.

**Confirm Settings and Create the Organization Virtual Datacenter**

Before you create the organization virtual datacenter, review the settings you entered.

**Procedure**

1  Review the settings for the organization virtual datacenter.
2  (Optional) Click **Back** to modify the settings.
3  (Optional) Select **Add networks to this organization after this wizard is finished** to immediately create an organization virtual datacenter network for this virtual datacenter.
4  Click **Finish** to accept the settings and create the organization virtual datacenter.
   When you create an organization virtual datacenter, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.

**Create an Organization Virtual Data Center from a Template**

You can create a new organization virtual data center from a virtual data center template that the organization has access to.
Prerequisites

Verify that the organization you want to create the organization virtual data center on is on the virtual data center template's access list.

Procedure

1. In the organization you want to create the new organization virtual data center in, click My Cloud and click Organization VDC Templates in the left pane.
2. Right-click the virtual data center to instantiate and click Instantiate.
3. Type a Name and optional Description for the new organization virtual data center and click Finish.

Enable or Disable an Organization Virtual Datacenter

You can disable an organization virtual datacenter to prevent the use of its compute and storage resources by other vApps and virtual machines. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Right-click the organization virtual datacenter name and select Enable or Disable.

Delete an Organization Virtual Datacenter

You can delete an organization virtual datacenter to remove its compute, memory, and storage resources from the organization. The resources remain unaffected in the source provider virtual datacenter.

Prerequisites

Disable the organization virtual datacenter and move or delete all of its vApps, vApp templates, and media.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Right-click the organization virtual datacenter name and select Delete.
3. Click Yes.

Organization Virtual Datacenter Properties

You can edit the properties of an existing organization virtual datacenter, including the virtual datacenter name and description, allocation model settings, storage settings, and network settings. You can also convert any VCDNI network pools used by the organization virtual datacenter to VXLAN pools.

See Network Pool and Services for details about VXLAN conversion.
Modify an Organization Virtual Datacenter Name and Description
As your vCloud Director installation grows, you might want to assign a more meaningful name or description to an existing organization virtual datacenter.

Edit Organization Virtual Datacenter Allocation Model Settings
You cannot change the allocation model for an organization virtual datacenter, but you can change some of the settings of the allocation model that you specified when you created the organization virtual datacenter.

Edit Organization Virtual Datacenter Storage Settings
After you create and use an organization virtual datacenter, you can provide it with more storage resources from its provider virtual datacenter. You can also enable or disable thin provisioning and fast provisioning for the organization virtual datacenter.

Edit Organization Virtual Datacenter Network Settings
You can change the maximum number of provisioned networks in an organization virtual datacenter and the network pool from which the networks are provisioned.

Modify an Organization Virtual Datacenter Name and Description
As your vCloud Director installation grows, you might want to assign a more meaningful name or description to an existing organization virtual datacenter.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Right-click the organization virtual datacenter name and select Properties.
3. On the General tab, type a new name and description and click OK.

You can use the name and description fields to indicate the vSphere functions available to the organization virtual datacenter, for example, vSphere HA.

Edit Organization Virtual Datacenter Allocation Model Settings
You cannot change the allocation model for an organization virtual datacenter, but you can change some of the settings of the allocation model that you specified when you created the organization virtual datacenter.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Right-click the organization virtual datacenter name and select Properties.
3 On the Allocation tab, enter the new allocation model settings and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100%. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization virtual datacenter are assigned this amount of GHz per vCPU. This option is available only for a Pay-As-You-Go allocation model.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100%. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

These settings affect only vApps that you start from this point on. vApps that are already running are not affected. The usage information that vCloud Director reports for this organization virtual datacenter does not reflect the new settings until all running vApps are stopped and started again.

Edit Organization Virtual Datacenter Storage Settings

After you create and use an organization virtual datacenter, you can provide it with more storage resources from its provider virtual datacenter. You can also enable or disable thin provisioning and fast provisioning for the organization virtual datacenter.

Fast provisioning requires a provider virtual datacenter backed by VMware vSphere® 5.0 or later. For information about fast provisioning, see Fast Provisioning of Virtual Machines.

Procedure
1 Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2 Right-click the organization virtual datacenter name and select Properties.
3 Click the Storage tab.
4 (Optional) Select Enable thin provisioning to enable thin provisioning for virtual machines in the organization virtual datacenter.
5 (Optional) Select Enable fast provisioning to enable fast provisioning for virtual machines in the organization virtual datacenter.
6 Click OK.
Edit Organization Virtual Datacenter Network Settings
You can change the maximum number of provisioned networks in an organization virtual datacenter and the network pool from which the networks are provisioned.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Right-click the organization virtual datacenter name and select Properties.
3. Click the Network Pool tab.
4. (Optional) Select a network pool from the drop-down menu or select None.
   If you select None, you can add a network pool later.
5. (Optional) Enter the maximum number of networks that the organization can provision from the network pool.
6. Click OK.

Add a Storage Policy to an Organization Virtual Datacenter
Add a storage policy to an organization virtual datacenter to support the storage policy for virtual machines on the provider virtual datacenter.

Prerequisites
One or more storage policies must be associated with the provider virtual datacenter that backs the organization virtual datacenter. See Add a VM Storage Policy to a Provider Virtual Data Center.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Storage Policies tab and click Add.
4. Select a storage policy, click Add and click OK.

Support for the storage policy is added to the organization virtual datacenter.

Managing Organization Virtual Data Center Templates
An organization virtual datacenter template specifies a configuration for an organization virtual data center and, optionally, an Edge Gateway and organization virtual data center network. System administrators who want to enable organization administrators to create these resources in their organization can create organization virtual data center templates and share them with those organizations.
By creating and sharing virtual data center templates, system administrators can enable self-service provisioning of organization virtual data centers while retaining administrative control over allocation of system resources such as provider virtual data centers and external networks. Organization administrators, or any role that has rights to view and instantiate VDC templates, use an instantiation operation to create organization virtual data centers from templates.

**Related Videos**

- Creating and Using VDC Templates
  (http://link.brightcove.com/services/player/bcid2296383276001?bctid=ref:video_vcd_vdc_templates)

- Create an Organization Virtual Data Center Template
  Create an organization virtual data center template to enable self-service provisioning of organization virtual data centers while retaining administrative control over allocation of system resources such as provider virtual data centers and external networks.

- Instantiate an Organization Virtual Data Center Template
  Instantiate a virtual data center template to create a new organization virtual data center from the virtual data center template.

- Modify an Organization Virtual Data Center Template
  You can edit the properties of an existing virtual data center template, including the name and description, allocation model settings, storage settings, and network settings.

- Clone an Organization Virtual Data Center Template
  Clone a virtual data center template to create a new virtual data center template based on an existing virtual data center template.

- Delete an Organization Virtual Data Center Template
  You can delete a virtual data center template from the system. Deleting a virtual data center template does not affect any virtual data centers that have already been created from the template.

**Create an Organization Virtual Data Center Template**

Create an organization virtual data center template to enable self-service provisioning of organization virtual data centers while retaining administrative control over allocation of system resources such as provider virtual data centers and external networks.

**Prerequisites**

Verify that you are logged in to vCloud Director as a system administrator.

**Procedure**

1. Open the New VDC Template Wizard
   Open the New VDC Template wizard to begin the process of creating an organization virtual data center template.
Select a Provider Virtual Data Center and External Network
An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

Select an Allocation Model
The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

Configure the Allocation Model
Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

Configure Storage Profiles
An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual data center datastores.

Configure the Network Pool
A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks. You can configure a virtual data center template to automatically connect to a network pool upon instantiation or to connect to no network pool.

Configure the Edge Gateway
Configure an edge gateway to enable routed networking in organization VDCs created from the template.

Configure Network Settings on a New Edge Gateway
Configure IP settings for external networks on the new edge gateway.

Configure the Access List
Add organizations to the virtual data center template access list to allow those organizations to instantiate virtual data centers from the template.

Name the Organization Virtual Data Center Template
Provide a descriptive name and optional description for the virtual data center to use in the system and in each organization that has access to the template.

Confirm the Organization Virtual Data Center Template Settings
Review and confirm the settings you entered for the virtual data center template.

Open the New VDC Template Wizard
Open the New VDC Template wizard to begin the process of creating an organization virtual data center template.

Procedure
1. Click the Manage & Monitor tab and click Organization VDC Templates in the left pane.
2. Click the add button.
Select a Provider Virtual Data Center and External Network

An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

Procedure

1. Select a provider virtual data center and external network pair from the top list and click **Add** to add the provider virtual data center and external network to the virtual data center template.

   Organization virtual data centers based on this template use the selected provider virtual data centers and external network. You can configure only one external network for each provider virtual data center.

2. (Optional) Select a provider virtual data center and external network pair from the bottom list and click **Remove** to remove the provider virtual data center and external network from the virtual data center template.

3. Click **Next**.

Select an Allocation Model

The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

Prerequisites

Verify that you understand which allocation model is appropriate for your environment. See Understanding Allocation Models.

Procedure

1. Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>A percentage of the resources you allocate from the provider virtual datacenter are committed to the organization virtual datacenter. You can specify the percentage for both CPU and memory.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are committed only when users create vApps in the organization virtual datacenter.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

For information about the placement engine and virtual machine shares, rates and limits, see the vCloud Director User's Guide.

2. Click **Next**.
Configure the Allocation Model

Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

Procedure

1. Select the allocation model options.

   Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default value for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the CPU allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization virtual datacenter are assigned this amount of GHz per vCPU. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the memory allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

2. Click Next.

Example: Configuring an Allocation Model

When you create an organization virtual datacenter, vCloud Director creates a vSphere resource pool based on the allocation model settings you specify.
Table 5-6. How Allocation Pool Settings Affect Resource Pool Settings When Single Cluster Allocation Pool is Enabled

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>25GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>50GB</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Table 5-7. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>Sum of the number of vCPU times vCPU frequency for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>Sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>Sum of the configured memory size for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>Sum of the configured memory size times the percentage guarantee for memory for all associated virtual machines</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Table 5-8. How Pay-As-You-Go Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation, CPU Limit</td>
<td>0.00GHz, Unlimited</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>100%</td>
<td>Memory Reservation, Memory Limit</td>
<td>0.00GB, Unlimited</td>
</tr>
</tbody>
</table>

Resource pools created to support Pay-As-You-Go organization virtual datacenters never have reservations or limits. Pay-As-You-Go settings affect only overcommitment. A 100 percent guarantee means overcommitment is impossible. The lower the percentage, the more overcommitment is possible.
Table 5-9. How Reservation Pool Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th>Reservation Pool Setting</th>
<th>Reservation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Configure Storage Profiles

An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual data center datastores.

Procedure

1. (Optional) Select a storage profile from the Available Storage Profiles list and click Add to add it to the virtual data center template.
   - Repeat this step to add multiple storage profiles.

2. (Optional) Select a storage profile from the Selected Storage Profiles list and click Remove to remove it from the virtual data center template.
   - Repeat this step to remove multiple storage profiles.

3. Verify that there is at least one storage profile in the Selected Storage Profiles list, and click Next.

Configure the Network Pool

A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks. You can configure a virtual data center template to automatically connect to a network pool upon instantiation or to connect to no network pool.

Procedure

1. Choose how the virtual data center connects to a network pool.
   - **Option**: Auto (Recommended)
     - Description: vCloud Director automatically connects the virtual data center to a network pool when you instantiate the template.
   - **Option**: None
     - Description: The virtual data center is not connected to a network pool when you instantiate the template.

2. Click Next.

Configure the Edge Gateway

Configure an edge gateway to enable routed networking in organization VDCs created from the template.

Procedure

1. (Optional) Select Create a new edge gateway to create and configure an edge gateway in the template.
2 Type a name and optional description for the new edge gateway.

3 Select a configuration for the edge gateway.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>Requires less memory and compute resources.</td>
</tr>
<tr>
<td>Large</td>
<td>Provides increased capacity and performance than with the Compact option. Large and X-Large configurations provide identical security functions.</td>
</tr>
<tr>
<td>X-Large</td>
<td>Suited for environments that have a load balancer with a large number of concurrent sessions.</td>
</tr>
<tr>
<td>Quad Large</td>
<td>Recommended for high throughput and requires a high connection rate.</td>
</tr>
</tbody>
</table>

This option appears only if you chose to create a new edge gateway. For more information on system requirements for deploying an edge gateway, see System Requirements for NSX in the NSX Administration Guide.

4 Select **Enable High Availability** to enable automatic failover to a backup gateway.

5 Select **Use default gateway for DNS relay** to use the selected default gateway for DNS relay.

6 Click **Next**.

**Configure Network Settings on a New Edge Gateway**
Configure IP settings for external networks on the new edge gateway.

This page appears only if you selected **Create a new edge gateway** during gateway configuration.

**Procedure**

1 On the **Configure IP Settings** page, click **Change IP Assignment**.

2 Select **Manual** from the drop-down menu for each external network for which to specify an IP address.

3 Type an IP address for each external network set to **Manual** and click **Next**.

**Configure the Access List**
Add organizations to the virtual data center template access list to allow those organizations to instantiate virtual data centers from the template.

**Procedure**

1 Select an organization from the **Available Organizations** list and click **Add** to add the organization to the virtual data center template access list.

   Repeat this step to add multiple organizations to the access list.

2 Select an organization from the **Selected Organizations** list and click **Remove** to remove the organization from the virtual data center access list.

   Repeat this step to remove multiple organizations from the access list.

3 Click **Next**.
Name the Organization Virtual Data Center Template

Provide a descriptive name and optional description for the virtual data center to use in the system and in each organization that has access to the template.

Procedure

1. Type a **System Name** for the virtual data center template.
   - This is the name that appears in the system's virtual data center templates list.
2. (Optional) Type a **System Description** for the virtual data center template.
   - This is the description that appears in the system's virtual data center template's list.
3. Type a **Tenant Name** for the virtual data center template.
4. (Optional) Type a **Tenant Description** for the virtual data center if you want a different description than the system description to appear on organizations with access to the virtual data center template.
5. Click **Next**.

Confirm the Organization Virtual Data Center Template Settings

Review and confirm the settings you entered for the virtual data center template.

Procedure

1. Review the settings for the virtual data center template.
2. (Optional) Click **Back** to modify the settings.
3. Click **Finish**.

Instantiate an Organization Virtual Data Center Template

Instantiate a virtual data center template to create a new organization virtual data center from the virtual data center template.

Prerequisites

Verify that the organization on which you want to create the new organization virtual data center has access to the virtual data center template.

Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDC Templates** in the left pane.
2. Right-click the virtual data center to instantiate and click **Instantiate**.
3. Type a **Name** and optional **Description** for the new organization virtual data center and click **Finish**.
Modify an Organization Virtual Data Center Template

You can edit the properties of an existing virtual data center template, including the name and description, allocation model settings, storage settings, and network settings.

Procedure

1. **Open the Edit New VDC Template Wizard**
   - Open the Edit VDC Template wizard to begin the process of modifying a virtual data center template.

2. **Select a Provider Virtual Data Center and External Network**
   - An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

3. **Select an Allocation Model**
   - The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

4. **Configure the Allocation Model**
   - Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

5. **Configure Storage Profiles**
   - An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual data center datastores.

6. **Configure the Network Pool**
   - A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks. You can configure a virtual data center template to automatically connect to a network pool upon instantiation or to connect to no network pool.

7. **Configure the Edge Gateway**
   - Configure an edge gateway to enable routed networking in organization VDCs created from the template.

8. **Configure Network Settings on a New Edge Gateway**
   - Configure IP settings for external networks on the new edge gateway.

9. **Configure the Access List**
   - Add organizations to the virtual data center template access list to allow those organizations to instantiate virtual data centers from the template.

10. **Name the Organization Virtual Data Center Template**
    - Provide a descriptive name and optional description for the virtual data center to use in the system and in each organization that has access to the template.

11. **Confirm the Organization Virtual Data Center Template Settings**
    - Review and confirm the settings you entered for the virtual data center template.
Open the Edit New VDC Template Wizard

Open the Edit VDC Template wizard to begin the process of modifying a virtual data center template.

Procedure

1. Click the Manage & Monitor tab and click Organization VDC Templates in the left pane.
2. Right-click the virtual data center template to modify, and select Properties.

Select a Provider Virtual Data Center and External Network

An organization virtual datacenter obtains its compute and storage resources from a provider virtual datacenter. The organization virtual datacenter provides these resources to vApps and virtual machines in the organization.

Procedure

1. Select a provider virtual data center and external network pair from the top list and click Add to add the provider virtual data center and external network to the virtual data center template.

   Organization virtual data centers based on this template use the selected provider virtual data centers and external network. You can configure only one external network for each provider virtual data center.

2. (Optional) Select a provider virtual data center and external network pair from the bottom list and click Remove to remove the provider virtual data center and external network from the virtual data center template.

3. Click Next.

Select an Allocation Model

The allocation model determines how and when the provider virtual datacenter compute and memory resources that you allocate are committed to the organization virtual datacenter.

Prerequisites

Verify that you understand which allocation model is appropriate for your environment. See Understanding Allocation Models.
Procedure

1 Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>A percentage of the resources you allocate from the provider virtual datacenter are committed to the organization virtual datacenter. You can specify the percentage for both CPU and memory.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are committed only when users create vApps in the organization virtual datacenter.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

For information about the placement engine and virtual machine shares, rates and limits, see the *vCloud Director User's Guide*.

2 Click Next.

**Configure the Allocation Model**

Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

Procedure

1 Select the allocation model options.

Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default value for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the CPU allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization virtual datacenter are assigned this amount of GHz per vCPU. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization virtual datacenter. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization virtual datacenter. You can overcommit resources by guaranteeing less than 100 percent. This option is available only for Allocation Pool and Pay-As-You-Go allocation models. The default for Allocation Pool is 50 percent, and the default for Pay-As-You-Go is 20 percent. For an Allocation Pool allocation model, the percentage guarantee also determines what percentage of the memory allocation is committed for this organization virtual datacenter.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the organization virtual datacenter.</td>
</tr>
</tbody>
</table>

2. Click **Next**.

**Example: Configuring an Allocation Model**

When you create an organization virtual datacenter, vCloud Director creates a vSphere resource pool based on the allocation model settings you specify.

**Table 5-10. How Allocation Pool Settings Affect Resource Pool Settings When Single Cluster Allocation Pool is Enabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>25GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>50GB</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>10GB</td>
</tr>
</tbody>
</table>

**Table 5-11. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled**

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>Sum of the number of vCPU times vCPU frequency for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>Sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>2.5GHz</td>
</tr>
</tbody>
</table>

vCloud Director Administrator's Guide

VMware, Inc. 84
Table 5-11. How Allocation Pool Settings Affect Resource Pool Settings When the Single Cluster Allocation Pool feature is Disabled (Continued)

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Sub-Resource Pool Value</th>
<th>Committed Value for this Org VDC Across All Subresource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Limit</td>
<td>Sum of the configured memory size for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>Sum of the configured memory size times the percentage guarantee for memory for all associated virtual machines</td>
<td>10GB</td>
</tr>
</tbody>
</table>

Table 5-12. How Pay-As-You-Go Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation, CPU Limit</td>
<td>0.00GHz, Unlimited</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>100%</td>
<td>Memory Reservation, Memory Limit</td>
<td>0.00GB, Unlimited</td>
</tr>
</tbody>
</table>

Resource pools created to support Pay-As-You-Go organization virtual datacenters never have reservations or limits. Pay-As-You-Go settings affect only overcommitment. A 100 percent guarantee means overcommitment is impossible. The lower the percentage, the more overcommitment is possible.

Table 5-13. How Reservation Pool Settings Affect Resource Pool Settings

<table>
<thead>
<tr>
<th>Reservation Pool Setting</th>
<th>Reservation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Configure Storage Profiles

An organization virtual datacenter requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider virtual data center datastores.

Procedure

1. (Optional) Select a storage profile from the Available Storage Profiles list and click Add to add it to the virtual data center template.

   Repeat this step to add multiple storage profiles.

2. (Optional) Select a storage profile from the Selected Storage Profiles list and click Remove to remove it from the virtual data center template.

   Repeat this step to remove multiple storage profiles.

3. Verify that there is at least one storage profile in the Selected Storage Profiles list, and click Next.
Configure the Network Pool

A network pool is a group of undifferentiated networks used to create vApp networks and internal organization virtual datacenter networks. You can configure a virtual data center template to automatically connect to a network pool upon instantiation or to connect to no network pool.

Procedure

1. Choose how the virtual data center connects to a network pool.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto (Recommended)</td>
<td>vCloud Director automatically connects the virtual data center to a network pool when you instantiate the template.</td>
</tr>
<tr>
<td>None</td>
<td>The virtual data center is not connected to a network pool when you instantiate the template.</td>
</tr>
</tbody>
</table>

2. Click Next.

Configure the Edge Gateway

Configure an edge gateway to enable routed networking in organization VDCs created from the template.

Procedure

1. (Optional) Select Create a new edge gateway to create and configure an edge gateway in the template.

2. Type a name and optional description for the new edge gateway.

3. Select a configuration for the edge gateway.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>Requires less memory and compute resources.</td>
</tr>
<tr>
<td>Large</td>
<td>Provides increased capacity and performance than with the Compact option. Large and X-Large configurations provide identical security functions.</td>
</tr>
<tr>
<td>X-Large</td>
<td>Suited for environments that have a load balancer with a large number of concurrent sessions.</td>
</tr>
<tr>
<td>Quad Large</td>
<td>Recommended for high throughput and requires a high connection rate.</td>
</tr>
</tbody>
</table>

This option appears only if you chose to create a new edge gateway. For more information on system requirements for deploying an edge gateway, see System Requirements for NSX in the NSX Administration Guide.

4. Select Enable High Availability to enable automatic failover to a backup gateway.

5. Select Use default gateway for DNS relay to use the selected default gateway for DNS relay.

6. Click Next.

Configure Network Settings on a New Edge Gateway

Configure IP settings for external networks on the new edge gateway.
This page appears only if you selected **Create a new edge gateway** during gateway configuration.

**Procedure**

1. On the **Configure IP Settings** page, click **Change IP Assignment**.
2. Select **Manual** from the drop-down menu for each external network for which to specify an IP address.
3. Type an IP address for each external network set to **Manual** and click **Next**.

**Configure the Access List**

Add organizations to the virtual data center template access list to allow those organizations to instantiate virtual data centers from the template.

**Procedure**

1. Select an organization from the **Available Organizations** list and click **Add** to add the organization to the virtual data center template access list.
   
   Repeat this step to add multiple organizations to the access list.
2. Select an organization from the **Selected Organizations** list and click **Remove** to remove the organization from the virtual data center access list.
   
   Repeat this step to remove multiple organizations from the access list.
3. Click **Next**.

**Name the Organization Virtual Data Center Template**

Provide a descriptive name and optional description for the virtual data center to use in the system and in each organization that has access to the template.

**Procedure**

1. Type a **System Name** for the virtual data center template.
   
   This is the name that appears in the system's virtual data center templates list.
2. (Optional) Type a **System Description** for the virtual data center template.
   
   This is the description that appears in the system's virtual data center template's list.
3. Type a **Tenant Name** for the virtual data center template.
4. (Optional) Type a **Tenant Description** for the virtual data center if you want a different description than the system description to appear on organizations with access to the virtual data center template.
5. Click **Next**.

**Confirm the Organization Virtual Data Center Template Settings**

Review and confirm the settings you entered for the virtual data center template.
Procedure
1 Review the settings for the virtual data center template.
2 (Optional) Click Back to modify the settings.
3 Click Finish.

Clone an Organization Virtual Data Center Template
Clone a virtual data center template to create a new virtual data center template based on an existing virtual data center template.

Procedure
1 Click the Manage & Monitor tab and click Organization VDC Templates in the left pane.
2 Right-click the virtual data center to instantiate and click Clone.
3 Click Name this VDC Template in the left pane, and type a System Name for the new virtual data center template.
4 (Optional) Click any of the settings in the left pane to modify that setting.
   The new virtual data center template retains the settings from the original virtual data center template for any settings you do not modify.
5 Click Finish.

Delete an Organization Virtual Data Center Template
You can delete a virtual data center template from the system. Deleting a virtual data center template does not affect any virtual data centers that have already been created from the template.

Procedure
1 Click the Manage & Monitor tab and click Organization VDC Templates in the left pane.
2 Right-click the virtual data center to delete and click Delete.

Managing External Networks
After you create an external network, you can add or remove network specifications, add or remove backing vSphere networks, and modify most other network properties.

Modify an External Network Name and Description
As your vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing external network.

Procedure
1 Click the Manage & Monitor tab and click External Networks in the left pane.
2 Right-click the external network name and select Properties.
3 On the Name and Description tab, type a new name and description and click OK.

View and Modify External Network Specifications

You can view, modify, or delete existing external network specifications and add new external network specifications.

- **Add a New External Network Specification**
  Add a new external network specification if you need an external networks specification with a different netmask or gateway than existing external network specifications have.

- **Modify an External Network Specification**
  If the network specification for an external network changes, you can modify its network settings.

Procedure

1 Click the Manage & Monitor tab and click External Networks in the left pane.
2 Right-click the external network name and select Properties.
3 Click the Network Specification tab.

Add a New External Network Specification

Add a new external network specification if you need an external networks specification with a different netmask or gateway than existing external network specifications have.

Procedure

1 Click the Manage & Monitor tab and click External Networks in the left pane.
2 Right-click the external network name and select Properties.
3 On the Network Specification tab, click Add.
4 Type the Gateway address and Subnet Mask for the external network specification to use.
5 (Optional) Type a Primary DNS and Secondary DNS for the external network specification to use.
6 Type one or more Static IP Pools for the external network specification to use.
   Separate multiple static IP pools with a carriage return.
7 Click OK.

Modify an External Network Specification

If the network specification for an external network changes, you can modify its network settings.

Procedure

1 Click the Manage & Monitor tab and click External Networks in the left pane.
2 Right-click the external network name and select Properties.
3 On the Network Specification tab, select the external network specification to modify, and click Modify.
Modify the settings as necessary and click OK.

You cannot modify the network mask or default gateway. If you need an external network with a different netmask or gateway, create one.

Edit the vSphere Network Backings of an External Network

If your system includes multiple vCenter servers and vSphere networks, you can edit the set of vSphere networks that back an external network.

Procedure

1. Click the Manage & Monitor tab and click External Networks in the left pane.
2. Right-click an external network and select Properties.
3. Click the vSphere Networks tab.
4. To modify the set of vSphere network that back this external network, click Edit.
5. If multiple vCenter servers are listed, select a vCenter server and vSphere network and click Add or Remove.
   All of the vSphere networks that back an external network must originate on the same type of switch: either DVSswitch or Standard switch. You can select only one vSphere network from each vCenter server. You cannot remove a backing network that is in use.
6. When you have finished editing the vCenter servers and vSphere networks that back this external network, click OK.

Add IP Addresses to an External Network IP Pool

If an external network is running out of IP addresses, you can add more addresses to its IP Pool.

Procedure

1. Click the Manage & Monitor tab and click External Networks in the left pane.
2. Right-click the external network name and select Properties.
3. On the Network Specification tab, select the subnet and click Modify.
4. Type an IP address or range of IP addresses in the text box.
5. Click OK, and click OK again.

Delete an External Network

Delete an external network to remove it from vCloud Director.

Prerequisites

Before you can delete an external network, you must delete all of the edge gateways and organization virtual datacenter networks that rely on it.
Procedure

1. Click the **Manage & Monitor** tab and click **External Networks** in the left pane.
2. Right-click the external network name and select **Delete Network**.

Managing Edge Gateways

An edge gateway provides a routed organization virtual datacenter network with connectivity to external networks and can provide services such as load balancing, network address translation, and a firewall.

Edge gateways require NSX. For more information, see the NSX documentation.

Add an Edge Gateway

An edge gateway provides routing and other services to a routed organization virtual datacenter network.

Procedure

1. **Open the New Edge Gateway Wizard**
   
   Open the New Edge Gateway wizard to start the process of adding an edge gateway to an organization virtual datacenter.

2. **Select External Networks for a New Edge Gateway**
   
   Select the external networks that the edge gateway can connect to.

3. **Configure IP Settings on a New Edge Gateway**
   
   Configure IP settings for external networks on the new edge gateway.

4. **Suballocate IP Pools on a New Edge Gateway**
   
   Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.

5. **Configure Rate Limits on a New Edge Gateway**
   
   Configure the inbound and outbound rate limits for each external network on the edge gateway.

6. **Configure the Name and Description of a New Edge Gateway**
   
   Enter a name and optional description for the edge gateway.

7. **Review the Configuration of a New Edge Gateway**
   
   Review the configuration of an edge gateway before completing the add process.

Open the New Edge Gateway Wizard

Open the New Edge Gateway wizard to start the process of adding an edge gateway to an organization virtual datacenter.

Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3 Click the **Edge Gateways** tab and click the add button.

The New Edge Gateway wizard opens.

**Select Gateway and IP Configuration Options for a New Edge Gateway**

Configure the edge gateway to connect to one or more physical networks.

**Procedure**

1 Select an edge gateway configuration based on your system resources.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>Requires less memory and compute resources.</td>
</tr>
<tr>
<td>Large</td>
<td>Provides increased capacity and performance than with the Compact option. Large and X-Large configurations provide identical security functions.</td>
</tr>
<tr>
<td>X-Large</td>
<td>Suited for environments that have a load balancer with large numbers of concurrent sessions.</td>
</tr>
<tr>
<td>Quad Large</td>
<td>Recommended for high throughput and requires a high connection rate.</td>
</tr>
</tbody>
</table>

For more information on system requirements for deploying an edge gateway, see *System Requirements for NSX* in the *NSX Administration Guide*.

2 (Optional) Select **Enable High Availability** to enable automatic failover to a backup edge gateway.

3 (Optional) Select **Create as Advanced Gateway** to enable use of the vCloud Director Tenant Portal to configure NSX services on the gateway.

**Important** Existing vCloud API clients might not be able to complete some operations on an advanced Edge Gateway. See [http://kb.vmware.com/kb/2147625](http://kb.vmware.com/kb/2147625).

4 (Optional) Select **Enable Distributed Routing** to configure an advanced gateway to provide distributed logical routing.

This option is available only if you select **Create as Advanced Gateway**. When you enable Distributed Routing, you can create many more organization VDC networks on the gateway. Traffic on those networks is optimized for VM-to-VM communication.

5 (Optional) Select **Configure IP Settings** to manually configure the external interface's IP address.

6 (Optional) Select **Sub-Allocate IP Pools** to allocate a set of IP addresses for gateway services to use.

7 (Optional) Select **Configure Rate Limits** to choose the inbound and outbound rate limits for each externally connected interface.

8 Click **Next**.

**Select External Networks for a New Edge Gateway**

Select the external networks that the edge gateway can connect to.
Procedure

1  Select an external network from the list and click Add.
   Hold down Ctrl to select multiple networks.
2  Select a network to be the Default Gateway.
3  (Optional) Select Use default gateway for DNS Relay.
4  Click Next.

Configure IP Settings on a New Edge Gateway

Configure IP settings for external networks on the new edge gateway.
This page appears only if you selected Configure IP Settings during gateway configuration.

Procedure

1  On the Configure IP Settings page, click Change IP Assignment.
2  Select Manual from the drop-down menu for each external network for which to specify an IP address.
3  Type an IP address for each external network set to Manual and click Next.

Suballocate IP Pools on a New Edge Gateway

Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.
This page appears only if you selected Sub-Allocate IP Pools during gateway configuration.

Procedure

1  Select an external network and IP pool to suballocate.
2  Type an IP address or range of IP addresses within the IP pool range and click Add.
   Repeat this step to add multiple suballocated IP pools.
3  (Optional) Select a suballocated IP pool and click Modify to modify the IP address range of the suballocated IP pool.
4  (Optional) Select a suballocated IP pool and click Remove to remove the suballocated IP pool.
5  Click Next.

Configure Rate Limits on a New Edge Gateway

Configure the inbound and outbound rate limits for each external network on the edge gateway.
This page appears only if you selected Configure Rate Limits during gateway configuration. Rate limits apply only to external networks backed by distributed port groups with static binding.
Procedure

1. Click **Enable** for each external network on which to enable rate limits.
2. Type the **Incoming Rate Limit** in gigabits per second for each enabled external network.
3. Type the **Outgoing Rate Limit** in gigabits per second for each enabled external network and click **Next**.

**Configure the Name and Description of a New Edge Gateway**

Enter a name and optional description for the edge gateway.

Procedure

1. Type a **Name** for the edge gateway.
2. (Optional) Type a **Description** for the edge gateway.
3. Click **Next**.

**Review the Configuration of a New Edge Gateway**

Review the configuration of an edge gateway before completing the add process.

Procedure

1. Review the settings for the new edge gateway and verify they are correct.
2. (Optional) Click **Back** to make any changes.
3. Click **Finish**.

**Convert an Edge Gateway to an Advanced Gateway**

After you convert an Edge Gateway to an Advanced Gateway, you can use the vCloud Director Tenant Portal to configure NSX services on the gateway.

**Prerequisites**

You must be a system administrator or an organization administrator to convert an Edge Gateway to an Advanced Gateway.

Procedure

1. Click the **Manage & Monitor** tab and click **Edge Gateways** in the left pane.
2. On the **Edge Gateways** tab, right-click the Edge Gateway name and select **Convert to Advanced Gateway**.

   The system prompts you to confirm your choice, then converts the gateway.

**Important**  After you convert an Edge Gateway, existing vCloud API clients might not be able to complete some operations on the Edge Gateway. See [http://kb.vmware.com/kb/2147625](http://kb.vmware.com/kb/2147625).
Enable or Disable Distributed Routing on an Advanced Gateway

After you convert an Edge Gateway to an Advanced Gateway, you can enable the gateway to provide vCloud Director Distributed Routing.

When you enable vCloud Director Distributed Routing on an Edge Gateway, you can create many more organization VDC networks on the gateway. Traffic on those networks is optimized for VM-to-VM communication.

Prerequisites

- NSX installations used by vCloud Director must be configured with one or more NSX Controller nodes. See the vCloud Director Installation and Upgrade Guide.
- You must be either a system administrator or a user in a role that includes the Organization vDC Gateway: Enable Distributed Routing right.

Procedure

1. Click the Manage & Monitor tab and click Edge Gateways in the left pane.
2. On the Edge Gateways tab, right-click the Edge Gateway name and select Enable Distributed Routing.

   If distributed routing is already enabled, the Enable Distributed Routing choice is replaced by Disable Distributed Routing.

   The system prompts you to confirm your choice, then enables or disables the feature.

Configuring Edge Gateway Services

An organization administrator can configure services such as DHCP, firewall, network address translation (NAT), and VPN on an Edge Gateway. If the Edge Gateway has been converted to an Advanced Gateway, additional service configuration choices are available.

**Important** After you convert an Edge Gateway to an Advanced Gateway, you must use the vCloud Director Tenant Portal to configure NSX services on the gateway. When you right-click the Edge Gateway name and select Edge Gateway Services, vCloud Director opens the Configure NSX Edge Gateway Services page in the Tenant Portal. For information about NSX Edge Gateway Service configuration see the vCloud Director Tenant Portal Guide.

Subtopics of this topic apply to configuring services on an Edge Gateway that has not been converted to an Advanced Gateway.

Configure DHCP for an Edge Gateway

You can configure edge gateways to provide DHCP services to virtual machines connected to associated organization virtual datacenter networks.
Prerequisites

System administrators and organization administrators can configure DHCP.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the DHCP tab and select Enable DHCP.
5. Click Add and type a range of IP addresses.
6. Set the default lease time and maximum lease time or use the default values.
7. Click OK.

vCloud Director updates the edge gateway to provide DHCP services.

Note: If the DNS settings on a DHCP-enabled edge gateway are changed, the edge gateway no longer provides DHCP services. To correct this issue, disable and reenable DHCP on the edge gateway.

Add a Source NAT rule to an Edge Gateway

A source NAT rule translates the source IP address of outgoing packets on an organization virtual datacenter that are being sent to another organization virtual datacenter network or an external network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the NAT tab and click Add SNAT.
5. Select an organization virtual datacenter network to apply this rule on from the Apply to drop-down menu.
6. Type the original IP address or range of IP addresses to apply this rule on in the Original (Internal) source IP/range text box.
7. Type the IP address or range of IP addresses to translate the addresses of outgoing packets to in the Translated (External) source IP/range text box.
8. Select Enabled and click OK.

The IP addresses of outgoing packets on the organization virtual datacenter network are translated according to the specifications of the source NAT rule.
Add a Destination NAT rule to an Edge Gateway

A destination NAT rule translates the IP address and port of packets received by an organization virtual datacenter network coming from another organization virtual datacenter network or an external network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the NAT tab and click Add DNAT.
5. Select an external network or another organization virtual datacenter network to apply this rule on from the Apply to drop-down menu.
6. Type the original IP address or range of IP addresses to apply this rule on in the Original (External) IP/range text box.
7. Choose the Protocol to apply this rule on from the drop-down menu.
   To apply this rule on all protocols, select Any.
8. (Optional) Select an Original port to apply this rule to.
9. (Optional) Select an IMCP type to apply this rule to if this rule applies to IMCP.
10. Type the IP address or range of IP addresses for the destination addresses on inbound packets to be translated to in the Translated (Internal) IP/range text box.
11. (Optional) Select a port for inbound packets to be translated to from the Translated port drop-down menu.
12. Select Enabled, and click OK.

The destination IP address and port are translated according to the destination NAT rule's specifications.

Configure the Firewall for an Edge Gateway

Edge gateways provide firewall protection for incoming and outgoing sessions.

You can set the default firewall action to deny or allow all traffic. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the set default. See Add a Firewall Rule for an Edge Gateway

System administrators and organization administrators can configure edge gateway firewalls.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.

4 Click the **Firewall** tab and select **Enable firewall** to enable firewall services, or deselect it to disable firewall services.

5 Select the default firewall action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Blocks all traffic except when overridden by a firewall rule.</td>
</tr>
<tr>
<td>Allow</td>
<td>Allows all traffic except when overridden by a firewall rule.</td>
</tr>
</tbody>
</table>

6 (Optional) Select the **Log** check box to log events related to the default firewall action.

7 Click **OK**.

**Add a Firewall Rule for an Edge Gateway**

You can add firewall rules to an edge gateway that supports a firewall. You can create rules to allow or deny traffic that matches the rules to pass through the firewall.

For a firewall rule to be enforced, you must enable the firewall for the edge gateway. See **Configure the Firewall for an Edge Gateway**.

When you add a new firewall rule to an edge gateway, it appears at the bottom of the firewall rule list. For information about setting the order in which firewall rules are enforced, see **Reorder Firewall Rules for an Edge Gateway**.

System administrators and organization administrators can add firewall rules to an edge gateway.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name and select **Edge Gateway Services**.

4 Click the **Firewall** tab and click **Add**.

5 Type a name for the rule.

6 Type the traffic **Source**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Type a source IP address to apply this rule on.</td>
</tr>
<tr>
<td>Range of IP addresses</td>
<td>Type a range of source IP addresses to apply this rule on.</td>
</tr>
<tr>
<td>CIDR</td>
<td>Type the CIDR notation of traffic to apply this rule on.</td>
</tr>
<tr>
<td>internal</td>
<td>Apply this rule to all internal traffic.</td>
</tr>
<tr>
<td>external</td>
<td>Apply this rule to all external traffic.</td>
</tr>
<tr>
<td>any</td>
<td>Apply this rule to traffic from any source.</td>
</tr>
</tbody>
</table>
7 Select a **Source port** to apply this rule on from the drop-down menu.

8 Type the traffic **Destination**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Type a destination IP address to apply this rule on.</td>
</tr>
<tr>
<td>Range of IP addresses</td>
<td>Type a range of destination IP addresses to apply this rule on.</td>
</tr>
<tr>
<td>CIDR</td>
<td>Type the CIDR notation of traffic to apply this rule on.</td>
</tr>
<tr>
<td>internal</td>
<td>Apply this rule to all internal traffic.</td>
</tr>
<tr>
<td>external</td>
<td>Apply this rule to all external traffic.</td>
</tr>
<tr>
<td>any</td>
<td>Apply this rule to traffic with any destination.</td>
</tr>
</tbody>
</table>

9 Select the **Destination port** to apply this rule on from the drop-down menu.

10 Select the **Protocol** to apply this rule on from the drop-down menu.

11 Select the action.

A firewall rule can allow or deny traffic that matches the rule.

12 Select the **Enabled** check box.

13 (Optional) Select the **Log network traffic for firewall rule** check box.

If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.

14 Click **OK** and click **OK** again.

**Reorder Firewall Rules for an Edge Gateway**

Firewall rules are enforced in the order in which they appear in the firewall list. You can change the order of the rules in the list.

When you add a new firewall rule to an edge gateway, it appears at the bottom of the firewall rule list. To enforce the new rule before an existing rule, reorder the rules.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name and select **Edge Gateway Services**.

4 Click the **Firewall** tab.

5 Drag the firewall rules to establish the order in which the rules are applied.

6 Click **OK**.
Enable VPN for an Edge Gateway

You can enable VPN for organization virtual datacenters backed by an edge gateway and create a secure tunnel from one of those organization virtual datacenter networks to another network.

vCloud Director supports VPN between organization virtual datacenter networks backed by edge gateways and both organization virtual datacenter networks in the same organization and remote networks.

System administrators and organization administrators can enable VPN.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab and select Enable VPN.
5. (Optional) Click Configure Public IPs, type a public IP address, and click OK.
6. Click OK.

What to do next

Create a VPN tunnel between an organization virtual datacenter network backed by the edge gateway to another network.

Configure Public IPs for External Networks

You can configure a public IP address for external networks associated with an edge gateway.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab and click Configure Public IPs.
5. Type an IP address to act as the public IP address for each external network and click OK.

Creating VPN Tunnels on an Edge Gateway

You can create VPN tunnels between organization virtual datacenter networks on the same organization, between organization virtual datacenter networks on different organizations, and between an organization virtual datacenter network and an external network.
vCloud Director does not support multiple VPN tunnels between the same two edge gateways. If there is an existing tunnel between two 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.

Create a VPN Tunnel In an Organization for an Organization Virtual Datacenter Network Backed by an Edge Gateway

You can create a VPN tunnel between an organization virtual datacenter network that is backed by edge gateway and another organization virtual datacenter in the same organization.

System administrators and organization administrators can create VPN tunnels.

If a firewall is between the tunnel endpoints, you must configure it 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

Prerequisites

Verify that you have at least two routed organization virtual datacenter networks in the organization. One of these networks must be backed by the edge gateway. Both organization virtual datacenter networks must have VPN enabled.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a network in this organization from the drop-down menu and select local and peer networks.
7. Review the tunnel settings and click OK.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel Between Organizations

You must use the vCloud Director Tenant Portal to create a VPN tunnel between two organization virtual datacenter networks in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.

See "Advanced Networking Capabilities for vCloud Director Tenants" in the vCloud Director Tenant Portal Guide.
Create a VPN Tunnel From an Organization Virtual Datacenter Network Backed by an Edge Gateway to a Remote Network

You can create a VPN tunnel between an organization virtual datacenter network that is backed by an edge gateway and a remote network.

System administrators and organization administrators can create VPN tunnels.

If a firewall is between the tunnel endpoints, you must configure it 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

Prerequisites

Verify that you have a routed remote network that uses IPSec and an organization virtual datacenter network backed by an edge gateway.

Procedure

1. Click the Manage & Monitor tab, and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a remote network from the drop-down menu.
7. Select the local organization virtual datacenter network.
8. Type the peer settings.
9. Review the tunnel settings and click OK.

vCloud Director configures the organization peer network endpoint.

What to do next

Manually configure the remote peer network endpoint. See Display Peer Settings for a VPN Tunnel to a Remote Network.

Display Peer Settings for a VPN Tunnel to a Remote Network

After you create a VPN tunnel to a remote network, display the peer settings for the VPN tunnel and configure the remote network according to those settings.
Prerequisites

A VPN tunnel to a remote network. See Create a VPN Tunnel From an Organization Virtual Datacenter Network Backed by an Edge Gateway to a Remote Network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab.
5. Select the VPN tunnel to display peer settings for, and click Peer settings.

vCloud Director displays the peer settings to configure on the remote network.

What to do next

Configure the displayed peer settings on the remote network.

Edit VPN Settings

You can edit the settings of an existing VPN tunnel.

Prerequisites

A VPN tunnel on the edge gateway. See Creating VPN Tunnels on an Edge Gateway.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab.
5. Select the VPN tunnel to display peer settings for, and click Edit.
6. Modify the settings as appropriate and click OK.

Configure Static Routing on an Edge Gateway

You can configure an edge gateway to add static routes that allow traffic between vApp networks routed to organization virtual datacenter networks backed by the edge gateway.

Any static route that you create is automatically enabled. To disable a static route, you must remove it.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.

**What to do next**

Create static routes. See [Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network](#) and [Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks](#).

**Managing Load Balancer Service on an Edge Gateway**

Edge gateways provide load balancing for TCP, HTTP, and HTTPS traffic.

You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 809 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPS.

- **Add a Pool Server to an Edge Gateway**
  You can add a pool server to manage and share back-end servers flexibly and efficiently. A pool manages health check monitors and load balancer distribution methods.

- **Edit Pool Server Settings**
  You can edit the settings of an existing pool server.

- **Delete a Pool Server**
  You can delete a server pool from an edge gateway.

- **Add a Virtual Server to an Edge Gateway**
  A virtual server is a highly scalable and highly available server built on a cluster of servers called members.

- **Edit Virtual Server Settings**
  You can edit the settings of an existing virtual server.

- **Delete a Virtual Server**
  You can delete a virtual server from an edge gateway.

**Add a Pool Server to an Edge Gateway**

You can add a pool server to manage and share back-end servers flexibly and efficiently. A pool manages health check monitors and load balancer distribution methods.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.
4 On the Load Balancer tab, click Pool Servers and click Add.

5 Type a name and optionally a description for the pool server and click Next.

6 Click Enable for each service to support.

7 Select a balancing method from the drop-down menu for each enabled service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Hash</td>
<td>Selects a server based on a hash of the source and destination IP address of each packet.</td>
</tr>
<tr>
<td>Round Robin</td>
<td>Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed.</td>
</tr>
<tr>
<td>URI</td>
<td>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 ensures that a URI is always directed to the same server as long as no server goes up or down.</td>
</tr>
<tr>
<td>Least Connected</td>
<td>Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.</td>
</tr>
</tbody>
</table>

8 (Optional) Change the default port for each enabled service if necessary.

9 Click Next.

10 Change the monitor port if required for each service that is to be supported by this pool.

11 Select the health check mode from the drop-down menu for each service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Tests servers using SSLv3 client hello messages. The server is considered valid only when the response contains server hello messages.</td>
</tr>
<tr>
<td>HTTP</td>
<td>The GET / default method is used to detect server status. Only responses 2xx and 3xx are valid. Other responses (including a lack of response) indicate a server failure.</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP connection check.</td>
</tr>
</tbody>
</table>

12 (Optional) Change the default health check parameters if necessary.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Interval at which a server is pinged.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time within which a response from the server must be received.</td>
</tr>
<tr>
<td>Health Threshold</td>
<td>Number of consecutive successful health checks before a server is declared operational.</td>
</tr>
<tr>
<td>Unhealth Threshold</td>
<td>Number of consecutive unsuccessful health checks before a server is declared dead.</td>
</tr>
</tbody>
</table>

13 For HTTP, type the URI referenced in the HTTP ping requests.

14 Click Next.
15 Click **Add** to add a back-end server to the pool.

16 Type the IP address of the server.

17 Type the weight to indicate the ratio of how many requests are to be served by this back-end server.

18 Change the default port and monitor port for the server if required.

19 Click **OK**.

20 (Optional) Repeat Step 15 through Step 19 to add additional servers.

21 Click **Next**.

22 Verify that the settings for the pool server are correct and click **Finish**.

**Edit Pool Server Settings**

You can edit the settings of an existing pool server.

**Prerequisites**

There must be an existing pool server on the edge gateway. See *Add a Pool Server to an Edge Gateway*.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.

4 On the **Load Balancer** tab, click **Pool Servers**.

5 Select the pool server to modify and click **Edit**.

6 Make the appropriate changes and click **OK**.

**Delete a Pool Server**

You can delete a server pool from an edge gateway.

**Prerequisites**

Verify that no virtual servers are using this pool server.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.

4 On the **Load Balancer** tab, click **Pool Servers**.

5 Select the pool server and click **Delete**.
Add a Virtual Server to an Edge Gateway

A virtual server is a highly scalable and highly available server built on a cluster of servers called members.

Prerequisites

The edge gateway must have at least one pool server. See Add a Pool Server to an Edge Gateway.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
5. Type a name for the virtual server.
6. (Optional) Type a description for the virtual server.
7. Select an external network from the Applied on drop-down menu.
8. Type the IP address of the virtual server.
9. Select a pool from the drop-down menu to be associated with the virtual server.
10. In Services, select Enable for each service to be supported.
11. Change the default Port, Persistence Method, Cookie Name, and Cookie Mode values for each enabled service as required.
12. Click Enabled to enable the virtual server.
13. (Optional) Click Log network traffic for virtual server.
14. Click OK.

Edit Virtual Server Settings

You can edit the settings of an existing virtual server.

Prerequisites

There must be an existing virtual server on the edge gateway. See Add a Virtual Server to an Edge Gateway.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4 On the Load Balancer tab, click Virtual Servers.
5 Select the virtual server to modify and click Edit.
6 Make the appropriate changes and click OK.

Delete a Virtual Server
You can delete a virtual server from an edge gateway.

Procedure
1 Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3 Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4 On the Load Balancer tab, click Virtual Servers.
5 Select the virtual server and click Delete.

Editing Edge Gateway Properties
You can change the settings for an existing edge gateway, including high availability, external network settings, IP pools, and rate limits.

- Enable High Availability on an Edge Gateway
  You can configure an edge gateway for high availability.
- Configure External Networks on an Edge Gateway
  Add or remove external networks connected to an edge gateway.
- Configure External Network IP Settings on an Edge Gateway
  Change the IP address for external interfaces on an edge gateway.
- Suballocate IP Pools on an Edge Gateway
  Suballocate into multiple static IP pools the IP pools that the external networks on an edge gateway provide.
- Configure Rate Limits on an Edge Gateway
  Configure the inbound and outbound rate limits for each external network on the edge gateway.

Enable High Availability on an Edge Gateway
You can configure an edge gateway for high availability.

Procedure
1 Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3 Click the Edge Gateways tab, right-click the edge gateway name, and select Properties.
4 Click the **General** tab and select **Enable HA**.

**Configure External Networks on an Edge Gateway**
Add or remove external networks connected to an edge gateway.

**Procedure**
1. Click the **Manage & Monitor** tab, and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Properties**.
4. Click the **External Networks** tab.
5. (Optional) Select an external network from the top list and click **Add** to add the external network to the edge gateway.
   - Hold down Ctrl to select multiple networks.
6. (Optional) Select an external network from the top list and click **Remove** to remove the external network from the edge gateway.
   - Hold down Ctrl to select multiple networks.
7. Select a network to be the **Default Gateway**.
8. (Optional) Select **Use default gateway for DNS Relay**.
9. Click **OK**.

**Configure External Network IP Settings on an Edge Gateway**
Change the IP address for external interfaces on an edge gateway.

**Procedure**
1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Properties**.
4. Click the **Configure IP Settings** tab, and click **Change IP Assignment**.
5. Select **Manual** from the drop-down menu for each external network you want to specify an IP address for.
6. Type a new IP address for each external network set to **Manual**, and click **OK**.

**Suballocate IP Pools on an Edge Gateway**
Suballocate into multiple static IP pools the IP pools that the external networks on an edge gateway provide.
Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Properties**.
4. Click the **Sub-Allocate IP Pools** tab.
5. Select an external network and IP pool to suballocate.
6. (Optional) Type an IP address or range of IP addresses within the IP pool range and click **Add** to add a suballocated IP pool.
7. (Optional) Select a suballocated IP pool and click **Modify** to modify the IP address range of the suballocated IP pool.
8. (Optional) Select a suballocated IP pool and click **Remove** to remove the suballocated IP pool.
9. Click **OK**.

Configure Rate Limits on an Edge Gateway

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. Click the **Manage & Monitor** tab, and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Properties**.
4. Click the **Configure Rate Limits** tab.
5. Click **Enable** for each external network on which to enable rate limits.
6. Type the **Incoming Rate Limit** in gigabits per second for each enabled external network.
7. Type the **Outgoing Rate Limit** in gigabits per second for each enabled external network, and click **OK**.

Upgrade an Edge Gateway

Upgrade an existing edge gateway to improve gateway capacity and performance.

Prerequisites

If you are upgrading an edge gateway with Full configuration and High Availability enabled to Full-4 configuration, ensure that ESXi has at least 8 CPUs.

Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
Double-click the organization virtual datacenter name to open the organization virtual datacenter.

Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Upgrade**.

Edge gateways with Compact configuration are upgraded to Full configuration, and edge gateways with Full configuration are upgraded to Full-4 configuration.

**What to do next**

If you upgraded a Compact gateway to Full configuration, you can repeat the upgrade process to upgrade to a gateway with Full-4 configuration.

**Delete an Edge Gateway**

You can delete an edge gateway to remove it from the organization virtual datacenter.

**Prerequisites**

Delete any organization virtual datacenter networks that the edge gateway backs.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Delete**.

**View IP Use for an Edge Gateway**

You can view a list of IP addresses that external interfaces on an edge gateway are currently using.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Edge Gateways** tab, right-click the edge gateway name, and select **External IP Allocations**.

**Apply Syslog Server Settings to an Edge Gateway**

You can apply syslog server settings to an edge gateway to enable firewall rule logging.

Apply syslog server settings to any edge gateway that was created before the initial creation of those settings. Apply the syslog server settings to an edge gateway any time the settings are changed.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Synchronize syslog server settings**.

Click **Yes**.

**Managing Organization Virtual Datacenter Networks**

System administrators and organization administrators can add, delete, and modify routed and isolated organization virtual datacenter networks. Only a system administrator can add, delete, and modify a direct organization virtual datacenter network.

- **Adding Networks to an Organization Virtual Datacenter**
  Add a network to an organization virtual datacenter to enable its virtual machines to communicate with each other or to provide access to the Internet. A single organization virtual datacenter can have multiple networks.

- **View or Modify Organization VDC Network Properties**
  After you create an organization VDC network, you can modify its name, description, DNS settings, sharing, and static IP pools.

- **Configuring Organization Virtual Datacenter Network Services**
  You can configure services, such as DHCP, firewalls, network address translation (NAT), and VPN for certain organization virtual datacenter networks. Organization administrators can also configure some network services for their organization virtual datacenter networks.

- **Reset an Organization Virtual Datacenter Network**
  If the network services that are associated with an organization virtual datacenter network are not working as expected, you can reset the network. Network services include DHCP settings, firewall settings, and so on.

- **View vApps and vApp Templates That Use an Organization Virtual Datacenter Network**
  You can view a list of the all the vApps and vApp templates that include virtual machines with a NIC connected to an organization virtual datacenter network. You cannot delete an organization virtual datacenter network with connected vApps or vApp templates.

- **Delete an Organization Virtual Datacenter Network**
  You can delete an organization virtual datacenter network to remove it from the organization virtual datacenter.

- **View IP Use for an Organization Virtual Datacenter Network**
  You can view a list of IP addresses that are currently in use in an organization virtual datacenter network IP pool.

**Adding Networks to an Organization Virtual Datacenter**

Add a network to an organization virtual datacenter to enable its virtual machines to communicate with each other or to provide access to the Internet. A single organization virtual datacenter can have multiple networks.
Table 5-14. Types of Organization Virtual Datacenter Networks and Their Requirements

<table>
<thead>
<tr>
<th>Organization Virtual Datacenter Network Type</th>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct connection to an external network</td>
<td>Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network. This network provides direct layer 2 connectivity to machines outside of the organization. Virtual machines outside of this organization can connect to virtual machines within the organization directly.</td>
<td>An external network must be accessible to your organization.</td>
</tr>
<tr>
<td>Routed organization virtual datacenter network</td>
<td>Accessible only by this organization. Only virtual machines within this organization can connect to this network. This network provides controlled access to an external network. System administrators and organization administrators can configure network address translation (NAT) and firewall settings to make specific virtual machines accessible from the external network.</td>
<td>An Edge Gateway must exist in your organization VDC.</td>
</tr>
<tr>
<td>Isolated organization virtual datacenter network</td>
<td>Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network. This network provides an organization with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to virtual machines outside this organization or on other networks within this organization.</td>
<td>A network pool must exist in your organization VDC.</td>
</tr>
</tbody>
</table>

Create an Organization VDC Network with a Direct Connection

A system administrator can create an organization virtual datacenter network that connects directly to an external network. VMs on the organization can use the external network to connect to other networks, including the Internet.

Prerequisites

- This operation is restricted to system administrators.
- An external network is required. See Add an External Network

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization VDC name to open the VDC.
3. Click the Org VDC Networks tab and click Add Network.
4. Select Connect directly to an external network.
5. Select an external network and click Next.
6. Type a name and optional description.
7 (Optional) Select **Share this network with other VDCs in the organization** to make the network available to other VDCs in the organization.

8 Click **Next**.

9 Review the network settings

   Click **Finish** to accept the settings and create the network, or click **Back** to modify the settings.

**Create an Organization VDC Network With a Routed Connection**

An organization VDC network with a routed connection provides controlled access to machines and networks outside of the organization VDC. System administrators and organization administrators can configure network address translation (NAT) and firewall settings on the network’s Edge Gateway to make specific virtual machines in the VDC accessible from an external network.

**Prerequisites**

- This operation requires the rights included in the predefined Organization Administrator role or an equivalent set of rights.
- The organization VDC must include an Edge Gateway. See **Add an Edge Gateway**.

**Procedure**

1 On the **Administration** tab, click **Virtual Datacenters** in the left pane.

2 Double-click an organization VDC name to open the organization VDC.

3 Click the **Org VDC Networks** tab and click **Add Network**.

4 Select **Create a routed network by connecting to an existing edge gateway**.

   a (Optional) Select an Edge Gateway for this network to connect to.

      If the organization VDC includes more than one Edge Gateway, you must choose one to support the new network. To be able to support another routed network, the Edge Gateway must show a value of at least 1 in the **Available Networks** column.

   b (Optional) Specify connection details for the new network.

      If you select **Connect directly to an external network**, no other network properties can be configured. For routed networks that do not connect directly to an external network, you can specify other options that allow the network to take advantage of NSX networking features. See the **NSX Administration Guide** for more information about these features.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest VLAN Allowed</td>
<td>Select this option to enable tagging of guest VLANs on this network.</td>
</tr>
<tr>
<td>Create as subinterface</td>
<td>Select this option to create the network as a subinterface.</td>
</tr>
<tr>
<td>Create as distributed interface</td>
<td>Select this option to create the network on a distributed logical router connected to this Edge Gateway.</td>
</tr>
</tbody>
</table>

5 On the **Configure Network** page, type a **Gateway address** and **Network mask** for the new network.
6  (Optional) Configure DNS settings for the network.

If you want DNS services to be available to VMs that connect to this network, you can configure those settings now. You can update these settings later if you need to by editing the properties of this network.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use gateway DNS</td>
<td>This option, which configures the network to use the same DNS settings as the Edge Gateway, is available only if the gateway has the Use default gateway for DNS relay property enabled.</td>
</tr>
<tr>
<td>Primary DNS, Secondary DNS, DNS suffix</td>
<td>If you do not select Use gateway DNS, you can provide your own DNS configuration values</td>
</tr>
</tbody>
</table>

7  (Optional) Configure static IP addresses for this network.

If you want this network to reserve one or more addresses for assignment to VMs that require a static IP address, enter the address or range of addresses and click Add. Repeat this step to add multiple static IP pools.

8  Click Next.

9  Type a name and optional description for the network.

10 (Optional) Select Share this network with other VDCs in the organization to make the organization VDC network available in other VDCs in the organization.

11 (Optional) Create or update metadata for this object.

   See Create or Update Object Metadata.

12 Click OK to save your changes.

13 Click Next.

14 Review the network settings.

   Click Finish to accept the settings and create the network, or click Back to modify the settings.

Create an Isolated Organization VDC Network

An isolated organization VDC network provides an isolated, private network that machines in the organization VDC can connect to. This network provides no connectivity to machines outside this organization VDC.

**Prerequisites**

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

- The organization VDC must include a network pool. By default, all organization VDCs are created with a VXLAN network pool.

**Procedure**

1  On the Administration tab, click Virtual Datacenters in the left pane.
2 Double-click an organization VDC name to open the organization VDC.

3 Click the **Org VDC Networks** tab and click **Add Network**.

4 Select **Create an isolated network within this virtual datacenter**, then click **Next**.

5 On the **Configure Network** page, type a **Gateway address** and **Network mask** for the new network.

6 (Optional) Configure DNS settings for the network.

   If you want DNS services to be available to VMs that connect to this network, you can configure those settings now. You can update these settings later if you need to by editing the properties of this network.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use gateway DNS</strong></td>
<td>This option, which configures the network to use the same DNS settings as the Edge Gateway, is available only if the gateway has the <strong>Use default gateway for DNS relay</strong> property enabled.</td>
</tr>
<tr>
<td><strong>Primary DNS, Secondary DNS, DNS suffix</strong></td>
<td>If you do not select <strong>Use gateway DNS</strong>, you can provide your own DNS configuration values</td>
</tr>
</tbody>
</table>

7 (Optional) Configure static IP addresses for this network.

   If you want this network to reserve one or more addresses for assignment to VMs that require a static IP address, enter the address or range of addresses and click **Add**. Repeat this step to add multiple static IP pools.

8 Click **Next**.

9 Type a name and optional description for the network.

10 (Optional) Select **Share this network with other VDCs in the organization** to make the organization VDC network available in other VDCs in the organization.

11 (Optional) Create or update metadata for this object.

   **See Create or Update Object Metadata.**

12 Click **OK** to save your changes.

13 Click **Next**.

14 Review the network settings.

   Click **Finish** to accept the settings and create the network, or click **Back** to modify the settings.

### View or Modify Organization VDC Network Properties

After you create an organization VDC network, you can modify its name, description, DNS settings, sharing, and static IP pools.

**Prerequisites**

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

1. On the **Administration** tab, click **Virtual Datacenters** in the left pane.
2. Double-click an organization VDC name to open the VDC.
3. On the **Org VDC Networks** tab, right-click a network name and click **Properties** to open the **Network Properties** page.
4. (Optional) Modify network **General** properties.
   a. Type a name and optional description for the network.
   b. Select **Share this network with other VDCs in the organization** to make the network available in other VDCs in the organization.
5. (Optional) Modify the **Network Specification**.
   a. Modify DNS settings for the network.
      - **Use gateway DNS**: This option, which configures the network to use the same DNS settings as the Edge Gateway, is available only if the gateway has the **Use default gateway for DNS relay** property enabled.
      - **Primary DNS, Secondary DNS, DNS suffix**: If you do not select **Use gateway DNS**, you can provide your own DNS configuration values. Your system administrator can suggest appropriate values for networks in your organization.
   b. Modify the **Static IP pool** for this network.
      - If you want this network to reserve one or more addresses for assignment to VMs that require a static IP address, enter the address or range of addresses and click **Add**. Repeat this step to add multiple static IP pools.
6. (Optional) Create or update metadata for this object.
   - See [Create or Update Object Metadata](#).
7. Click **OK** to save your changes.

**Configuring Organization Virtual Datacenter Network Services**

You can configure services, such as DHCP, firewalls, network address translation (NAT), and VPN for certain organization virtual datacenter networks. Organization administrators can also configure some network services for their organization virtual datacenter networks.

Table 5-15 lists the network services that vCloud Director provides to each type of organization virtual datacenter network.
Table 5.15. Network Services Available by Network Type

<table>
<thead>
<tr>
<th>Network Type</th>
<th>DHCP</th>
<th>Firewall</th>
<th>NAT</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>External organization virtual datacenter network - direct connection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External organization virtual datacenter network - routed connection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internal organization virtual datacenter network</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure DHCP for an Organization Virtual Datacenter Network

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

vCloud Director assigns a DHCP IP address to a virtual machine when you power it on if you performed the following tasks:

- Enabled DHCP for an organization virtual datacenter network
- Connected to that network a NIC on a virtual machine in the organization
- Selected **DHCP** as the IP mode for that NIC

System administrators and organization administrators can configure DHCP.

**Prerequisites**

Verify that you have a routed organization virtual datacenter network or an internal organization virtual datacenter network.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.
4. Click the **DHCP** tab and select **Enable DHCP**.
5. Type a range of IP addresses or use the default range.
   - vCloud Director uses these addresses to satisfy DHCP requests. The range of DHCP IP addresses cannot overlap with the static IP pool for the organization virtual datacenter network.
6. Set the default lease time and maximum lease time or use the default values.
7. Click **OK**.

vCloud Director updates the network to provide DHCP services.
Enable the Firewall for an Organization Virtual Datacenter Network

You can configure certain organization virtual datacenter networks to provide firewall services. You can enable the firewall on an organization virtual datacenter network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

You can deny all incoming traffic, deny all outgoing traffic, or both. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the generic rules to deny all incoming or outgoing traffic. See Add a Firewall Rule for an Organization Virtual Datacenter Network.

System administrators and organization administrators can enable firewalls.

Prerequisites

Verify that you have an external routed organization virtual datacenter network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
4. Click the Firewall tab and select Enable firewall.
5. Select the default firewall action.
6. (Optional) Select the Log check box to log events related to the default firewall action.
7. Click OK.

Add a Firewall Rule for an Organization Virtual Datacenter Network

You can add firewall rules to an organization virtual datacenter network that supports a firewall. You can create rules to allow or deny traffic that matches the rules to pass through the firewall.

For a firewall rule to be enforced, you must enable the firewall for the organization virtual datacenter network. See Enable the Firewall for an Organization Virtual Datacenter Network.

When you add a new firewall rule to an organization virtual datacenter network, it appears at the bottom of the firewall rule list. For information about setting the order in which firewall rules are enforced, see Reorder Firewall Rules for an Organization Virtual Datacenter Network.

System administrators and organization administrators can add firewall rules.

Prerequisites

Verify that you have an external NAT-routed organization virtual datacenter network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
Double-click the organization virtual datacenter name to open the organization virtual datacenter.

Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.

Click the Firewall tab and click Add.

Type a name for the rule.

Select the traffic direction.

Type the source IP address and select the source port.

For incoming traffic, the source is the external network. For outgoing traffic, the source is the organization virtual datacenter network.

Type the destination IP address and select the destination port.

For incoming traffic, the destination is the organization virtual datacenter network. For outgoing traffic, the destination is the external network.

Select the protocol and action.

A firewall rule can allow or deny traffic that matches the rule.

Select the Enabled check box.

(Optional) Select the Log network traffic for firewall rule check box.

If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.

Click OK and click OK again.

Reorder Firewall Rules for an Organization Virtual Datacenter Network

Firewall rules are enforced in the order in which they appear in the firewall list. You can change the order of the rules in the list.

When you add a new firewall rule to an organization virtual datacenter network, it appears at the bottom of the firewall rule list. To enforce the new rule before an existing rule, reorder the rules.

Prerequisites

Verify that you have a routed organization virtual datacenter network with two or more firewall rules.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name and select Configure Services.
4. Click the Firewall tab.
5. Drag the firewall rules to establish the order in which the rules are applied.
Enable VPN for an Organization Virtual Datacenter Network

You can enable VPN for an organization virtual datacenter network and create a secure tunnel to another network.

vCloud Director supports VPN between organization virtual datacenter networks in the same organization, organization virtual datacenter networks in different organizations (including organization virtual datacenter networks in different instances of vCloud Director), and remote networks.

System administrators and organization administrators can enable VPN.

Prerequisites

Verify that you have an external routed organization virtual datacenter network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
4. Click the VPN tab and select Enable VPN.
5. (Optional) Click Configure Public IPs, type a public IP address, and click OK.
6. Click OK.

What to do next

Create a VPN tunnel to another network.

Create a VPN Tunnel Within an Organization

You can create a VPN tunnel between two organization virtual datacenter networks in the same organization.

Both system administrators and organization administrators can create VPN tunnels.

If a firewall is between the tunnel endpoints, you must configure it 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
Prerequisites

Verify that you have at least two routed organization virtual datacenter networks with non-overlapping IP subnets and VPN enabled on both networks.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a network in this organization from the drop-down menu and select a peer network.
7. Review the tunnel settings and click OK.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel to a Remote Network

You can create a VPN tunnel between an organization virtual datacenter network and a remote network. System administrators and organization administrators can create VPN tunnels.

If a firewall is between the tunnel endpoints, you must configure it 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

Prerequisites

Verify that you have a routed organization virtual datacenter network and a routed remote network that uses IPSec.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name and select Configure Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6 Select a remote network from the drop-down menu.

7 Type the peer settings.

   See VMware Knowledge Base article https://kb.vmware.com/kb/2051370.

8 Review the tunnel settings and click OK.

vCloud Director configures the organization peer network endpoint.

What to do next
Manually configure the remote peer network endpoint.

Configure Static Routing for an Organization Virtual Datacenter Network
You can configure certain organization virtual datacenter networks to add static routes to allow traffic between different vApp networks routed to the organization virtual datacenter network.

Any static route that you create is automatically enabled. To disable a static route, you must remove it.

Prerequisites
Verify that you have a routed organization virtual datacenter network.

Procedure
1 Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2 Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3 Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.

What to do next
Create static routes. See Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network and Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks.

Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network
You can add static routes between two vApp networks that are routed to the same organization virtual datacenter network. Static routes allow traffic between the networks.

You cannot add static routes between overlapping networks or fenced vApps. After you add a static route to an organization virtual datacenter network, configure the network firewall rules to allow traffic on the static route.

Static routes function only when the vApps included in the routes are running. If you perform any of the following operations on a vApp that includes static routes, the static routes no longer function and you must remove them manually.

- Change the parent network of a vApp
Delete a vApp
Delete a vApp network

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

Verify that the networks have the following configurations:
- A routed organization virtual datacenter network.
- Static routing is enabled on the organization virtual datacenter network.
- Two vApp networks are routed to the organization virtual datacenter network.
- The vApp networks are in vApps that were started at least once.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name and select Configure Services.
5. Type a name, network address, and next hop IP.
   - The network address is for the first vApp network to which to add a static route. The next hop IP is the external IP address of that vApp network's router.
6. Select Within this network and click OK.
7. Click OK.
8. Repeat steps Step 4 through Step 7 to add a route to the second vApp network.

Example: Static Routing Example
vApp Network 1 and vApp Network 2 are both routed to Org VDC Network Shared. You can create static routes on the organization virtual datacenter network to allow traffic between the vApp networks. You can use information about the vApp networks to create the static routes.

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network Specification</th>
<th>Router External IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>192.168.2.0/24</td>
<td>192.168.0.101</td>
</tr>
<tr>
<td>Org VDC Network Shared</td>
<td>192.168.0.0/24</td>
<td>NA</td>
</tr>
</tbody>
</table>

On Org VDC Network Shared, create a static route to vApp Network 1 and another static route to vApp Network 2.
Table 5.17. Static Routing Settings

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network</th>
<th>Next Hop IP Address</th>
<th>Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>tovapp1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
<td>Within this network</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>tovapp2</td>
<td>192.168.2.0/24</td>
<td>192.168.0.101</td>
<td>Within this network</td>
</tr>
</tbody>
</table>

What to do next

Create firewall rules to allow traffic on the static routes. See Add a Firewall Rule for an Organization Virtual Datacenter Network.

Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks

An organization administrator can add static routes between two vApp networks that are routed to different organization virtual datacenter networks. Static routes allow traffic between the networks.

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

Static routes function only when the vApps included in the routes are running. If a vApp includes static routes and you perform the following operations, the static routes cannot function and you must remove them manually.

- Change the parent network of the vApp
- Delete a vApp
- Delete a vApp network

Prerequisites

Verify that vCloud Director has the following configurations:

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

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
5 Type a name, network address, and next hop IP address.

The network address is for the vApp network to which to add a static route. The next hop IP address is the external IP address of the router for the organization virtual datacenter network to which that vApp network is routed.

6 Select **To external network** and click **OK**.

7 Click **Add**.

8 Type a name, network address, and next hop IP address.

The network address is for the vApp network that is routed to this organization virtual datacenter network. The next hop IP address is the external IP address of the router for that vApp network.

9 Select **Within this network** and click **OK**.

10 Repeat steps **Step 4** through **Step 9** to add static routes to the second organization virtual datacenter network.

**Example: Static Routing Example**

vApp Network 1 is routed to Org VDC Network 1. vApp Network 2 is routed to Org VDC Network 2. You can create static routes on the organization virtual datacenter networks to allow traffic between the vApp networks. You can use information about the vApp networks and organization virtual datacenter networks to create the static routes.

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network Specification</th>
<th>Router External IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>192.168.11.0/24</td>
<td>192.168.10.100</td>
</tr>
<tr>
<td>Org VDC Network 1</td>
<td>192.168.0.0/24</td>
<td>10.112.205.101</td>
</tr>
<tr>
<td>Org VDC Network 2</td>
<td>192.168.10.0/24</td>
<td>10.112.205.100</td>
</tr>
</tbody>
</table>

On Org VDC Network 1, create a static route to vApp Network 2 and another static route to vApp Network 1. On Org VDC Network 2, create a static route to vApp Network 1 and another static route to vApp Network 2.

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network</th>
<th>Next Hop IP Address</th>
<th>Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 2</td>
<td>tovapp2</td>
<td>192.168.11.0/24</td>
<td>10.112.205.100</td>
<td>To external network</td>
</tr>
<tr>
<td>vApp Network 1</td>
<td>tovapp1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
<td>Within this network</td>
</tr>
</tbody>
</table>
Table 5-20. Static Routing Settings for Org VDC Network 2

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network</th>
<th>Next Hop IP Address</th>
<th>Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>tovapp1</td>
<td>192.168.1.0/24</td>
<td>10.112.205.101</td>
<td>To external network</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>tovapp2</td>
<td>192.168.11.0/24</td>
<td>192.168.10.100</td>
<td>Within this network</td>
</tr>
</tbody>
</table>

What to do next

Create firewall rules to allow traffic on the static routes. See Add a Firewall Rule for an Organization Virtual Datacenter Network.

Reset an Organization Virtual Datacenter Network

If the network services that are associated with an organization virtual datacenter network are not working as expected, you can reset the network. Network services include DHCP settings, firewall settings, and so on.

Before you delete a provider virtual datacenter, reset the organization virtual datacenter networks that depend on it.

No network services are available while an organization virtual datacenter network resets.

Prerequisites

Verify that you have a routed organization virtual datacenter network or an internal organization virtual datacenter network.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Reset Network.
4. Click Yes.

View vApps and vApp Templates That Use an Organization Virtual Datacenter Network

You can view a list of all the vApps and vApp templates that include virtual machines with a NIC connected to an organization virtual datacenter network. You cannot delete an organization virtual datacenter network with connected vApps or vApp templates.

Procedure

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name and select **Connected vApps**.

4. Click **OK**.

### Delete an Organization Virtual Datacenter Network

You can delete an organization virtual datacenter network to remove it from the organization virtual datacenter.

#### Prerequisites

Verify that no virtual machines are connected to the organization virtual datacenter network. See **View vApps and vApp Templates That Use an Organization Virtual Datacenter Network**.

#### Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Delete**.

### View IP Use for an Organization Virtual Datacenter Network

You can view a list of IP addresses that are currently in use in an organization virtual datacenter network IP pool.

#### Procedure

1. Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **IP Allocations**.

### Managing Network Pools

After you create a network pool, you can modify its name or description, or delete it. Depending on the type of network pool, you can also add port groups, and VLAN IDs. You cannot modify or delete VXLAN network pools.

- **Modify a Network Pool Name and Description**
  As your vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing network pool.

- **Add a Port Group to a Network Pool**
  You can add port groups to a network pool that is backed by port groups.

- **Add VLAN IDs to a Network Pool**
  You can add VLAN IDs to a network pool that is backed by a VLAN.
Delete a Network Pool
Delete a network pool to remove it from vCloud Director. You cannot delete VXLAN network pools.

Modify a Network Pool Name and Description
As your vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing network pool.

Procedure
1. Click the Manage & Monitor tab and then click Network Pools in the left pane.
2. Right-click the network pool name and select Properties.
3. On the General tab, type a new name or description and click OK.

Add a Port Group to a Network Pool
You can add port groups to a network pool that is backed by port groups.

Prerequisites
- Verify that you have a network pool that is backed by a port group
- Verify that you have an available port group in vSphere

Procedure
1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Right-click the network pool name and select Properties.
3. On the Network Pool Settings tab, select a port group, click Add, and click OK.

Add VLAN IDs to a Network Pool
You can add VLAN IDs to a network pool that is backed by a VLAN.

Prerequisites
Verify that your system includes the following items:
- A network pool that is backed by a VLAN
- Available VLAN IDs in vSphere

Procedure
1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Right-click the network pool name and select Properties.
3. On the Network Pool Settings tab, type a VLAN ID range and click Add.
4. Select a vSphere distributed switch and click OK.
Delete a Network Pool

Delete a network pool to remove it from vCloud Director. You cannot delete VXLAN network pools.

Prerequisites

Verify that the following conditions exist:

- No organization virtual datacenter is associated with the network pool.
- No vApps use the network pool
- No organization virtual datacenter networks use the network pool.

Procedure

1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Right-click the network pool name and select Delete.
3. Click Yes.

Managing Cloud Cells

You manage cloud cells mostly from the vCloud Director server host on which the cell resides, but you can delete a cloud cell from the vCloud Director Web console.

Table 5-21 lists the basic commands for controlling a cloud cell.

Table 5-21. Cloud Cell Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service vmware-vcd start</td>
<td>Starts the cell</td>
</tr>
<tr>
<td>service vmware-vcd restart</td>
<td>Restarts the cell</td>
</tr>
<tr>
<td>service vmware-vcd stop</td>
<td>Stops the cell</td>
</tr>
</tbody>
</table>

When you stop a cell, you may want to display a maintenance message to users that attempt to access that cell using a browser or the vCloud API. See Turn On Cloud Cell Maintenance Message.

- Adding Cloud Cells
  
  To add cloud cells to a vCloud Director installation, install the vCloud Director software on additional Cloud Director server hosts in the same vCloud Director cluster.

- Delete a Cloud Cell
  
  If you want to remove a cloud cell from your vCloud Director installation, in order to reinstall the software, or for some other reason, you can delete the cell.

- Turn On Cloud Cell Maintenance Message
  
  If you want to stop a cell and let users know that you are performing maintenance, you can turn on the maintenance message.
Turn Off Cloud Cell Maintenance Message

When you finish performing maintenance on a cell and are ready to restart the cell, you can turn off the maintenance message.

Adding Cloud Cells

To add cloud cells to a vCloud Director installation, install the vCloud Director software on additional Cloud Director server hosts in the same vCloud Director cluster.

For more information, see the VMware vCloud Director Installation and Configuration Guide.

Delete a Cloud Cell

If you want to remove a cloud cell from your vCloud Director installation, in order to reinstall the software, or for some other reason, you can delete the cell.

You can also delete a cell if it becomes unreachable.

Prerequisites

You must stop the cell using the service vmware-vcd stop command.

Procedure

1. Click the Manage & Monitor tab and click Cloud Cells in the left pane.
2. Right-click the cell name and select Delete.

vCloud Director removes information about the cell from its database.

Turn On Cloud Cell Maintenance Message

If you want to stop a cell and let users know that you are performing maintenance, you can turn on the maintenance message.

When the maintenance message is turned on, users who try to log in to the cell from a browser see a message stating that the cell is unavailable because of maintenance. Users who try to reach the cell using the vCloud API receive a similar message.

Procedure

1. Stop the cell by running the service vmware-vcd stop command.
2. Run the /opt/vmware/vcloud-director/bin/vmware-vcd-cell maintenance command.

Users cannot access the cell by using a browser or the vCloud API.

Turn Off Cloud Cell Maintenance Message

When you finish performing maintenance on a cell and are ready to restart the cell, you can turn off the maintenance message.
Procedure

- Run the following command on the cell to turn off the maintenance message.
  
  ```
  [root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
  ```

Users can now access the cell by using a browser or the vCloud API.

Managing Service Offerings

Service offerings enable you to offer products and platforms as services in a virtual datacenter.

For the most recent information about compatibility between vCloud Director and other VMware products, see the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

To enable service offering integration, see Using the vCloud API to Enable and Configure vCloud Director Service Offering Integration.

- Register an Extension
  Register an extension to offer vFabric Data Director or Cloud Foundry services in vCloud Director.

- View or Modify Extension Properties
  You can view an extension's type and associated service offerings and modify an extension's properties, such as name, namespace, user name, and password.

- Associate a Service Offering With an Organization Virtual Datacenter
  You can associate extension services with organization virtual datacenters to make those services available to virtual machines on the virtual datacenter.

- Disassociate a Service Offering From an Organization Virtual Datacenter
  You can dissociate a service offering from an organization virtual datacenter to remove access to the service from virtual machines on the organization virtual datacenter.

- Unregister an Extension
  You can unregister an extension to remove access to its services from vCloud Director

- Create a Service Instance
  Create a service instance that can be used by virtual machines on the organization virtual datacenter.

- Modify Service Instance Properties
  You can change a service instance's properties, such as its name, description, and parameters.

- Add a Service Instance to a Virtual Machine
  You can add any service instance on an organization virtual datacenter to a virtual machine on the organization virtual datacenter.

- Delete a Service Instance
  You can delete a service instance from an organizational virtual datacenter.
Register an Extension

Register and extension to offer vFabric Data Director or Cloud Foundry services in vCloud Director.

Prerequisites

- Enable service offering integration in vCloud Director. See Using the vCloud API to Enable and Configure vCloud Director Service Offering Integration.
- Verify that you are using a supported version of vFabric Data Director or Cloud Foundry. See Managing Service Offerings.
- Verify that you have the URL or IP address of the vFabric Data Director or Cloud Foundry installation accessible.

Procedure

1. Click the Manage & Monitor tab and click Extensions.
2. Click Add.
3. Select the extension type from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Director</td>
<td>Register a VMware vFabric Data Director extension. vCloud Director supports VMware vFabric Data Director version 2.7 services.</td>
</tr>
<tr>
<td>Cloud Foundry</td>
<td>Register a Cloud Foundry extension. vCloud Director supports Cloud Foundry platform version 1.0 services.</td>
</tr>
</tbody>
</table>

4. Type the namespace for the extension.
5. Type name and optional description for the extension.
6. Type the URL or IP address of the vFabric Data Director or Cloud Foundry installation to use for the extension.
7. Type the user name and user password for the extension, and click OK.

What to do next

Associate the extension's service offerings with virtual datacenters. See Associate a Service Offering With an Organization Virtual Datacenter.

View or Modify Extension Properties

You can view an extension's type and associated service offerings and modify an extension's properties, such as name, namespace, user name, and password.

Procedure

1. Click the Manage & Monitor tab and click Extensions.
2. Right-click the extension and select Properties.
3 (Optional) Click the **General** tab and type any new settings for the extension.

4 (Optional) Click the **Service Offerings** tab to see the service offerings associated with the extension.

5 Click **OK**.

**Associate a Service Offering With an Organization Virtual Datacenter**

You can associate extension services with organization virtual datacenters to make those services available to virtual machines on the virtual datacenter.

**Prerequisites**

Register an extension with vCloud Director. See [Register an Extension](#).

**Procedure**

1 Click the **Manage & Monitor** tab and click **Extensions**.

2 Right-click the extension to associate a service offering from and select **Associate Service Offerings**.

3 Select the service offering to associate and click **Next**.

4 Select an organization virtual datacenter to associate with the service offering and click **Next**.

5 Review the service offering associations and click **Finish**.

**What to do next**

Create service instances for use by virtual machines on the organization virtual datacenter. See [Create a Service Instance](#).

**Disassociate a Service Offering From an Organization Virtual Datacenter**

You can dissociate a service offering from an organization virtual datacenter to remove access to the service from virtual machines on the organization virtual datacenter.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Extensions**.

2 Right-click the extension to associate a service offering from and select **Disassociate Service Offerings**.

3 Select the service offering to disassociate and click **Next**.

4 Select the organization virtual datacenter to disassociate the service offering from and click **Next**.

5 Review the service offering disassociations and click **Finish**.
Unregister an Extension

You can unregister an extension to remove access to its services from vCloud Director

Procedure
1. Click the Manage & Monitor tab and click Extensions.
2. Right-click the extension and select Unregister.
3. Click Yes.

Create a Service Instance

Create a service instance that can be used by virtual machines on the organization virtual datacenter.

Prerequisites

Associate service offerings with the organization virtual datacenter. See Associate a Service Offering With an Organization Virtual Datacenter.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs.
2. Right-click the organization virtual datacenter and select Open.
3. Click My Cloud and select Services in the left pane.
4. Click Add.
5. Select the service offering to use for this instance and click Next.
6. Type a value for each of the required service offering parameters and click Next.
7. Type a name and optional description for the service instance and click Next.
8. Review the service offering configurations and click Finish.

What to do next

Add the service instance to a virtual machine. See Add a Service Instance to a Virtual Machine.

Modify Service Instance Properties

You can change a service instance's properties, such as its name, description, and parameters.

Procedure
1. Click the Manage & Monitor tab and click Organization VDCs.
2. Right-click the organization virtual datacenter and select Open.
3. Click My Cloud and select Services in the left pane.
4. Right-click the service instance to delete and select Properties.
5  (Optional) Click **General** and type a new name and description for the service instance.

6  (Optional) Click **Parameters** and type new values for any of the service instance parameters.

7  Click **OK**.

**Add a Service Instance to a Virtual Machine**

You can add any service instance on an organization virtual datacenter to a virtual machine on the organization virtual datacenter.

**Prerequisites**

Create a service instance on the organization virtual datacenter. See [Create a Service Instance](#).

**Procedure**

1  Click the **Manage & Monitor** tab and click **Organization VDCs**.

2  Right-click the organization virtual datacenter and select **Open**.

3  Click **My Cloud** and select **VMs** in the left pane.

4  Right-click a virtual machine and select **Properties**.

5  Click the **Services** tab.

6  Select the service instance to add and click **Add**.

   When you select a service instance, its parameters appear at the bottom of the dialog box.

7  Click **OK**.

**Delete a Service Instance**

You can delete a service instance from an organizational virtual datacenter.

**Procedure**

1  Click the **Manage & Monitor** tab and click **Organization VDCs**.

2  Right-click the organization virtual datacenter and select **Open**.

3  Click **My Cloud** and select **Services** in the left pane.

4  Right-click the service instance to delete and select **Delete**.

5  Click **Yes**.

**Configuring and Managing Multisite Deployments**

The vCloud Director Multisite feature enables a service provider or other institutional owner of multiple, geographically-distributed vCloud Director installations (server groups) to manage and monitor those installations and their organizations as single entities.
When you associate two vCloud Director sites, you enable administration of the sites as a single entity. You 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 vCloud 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. The vCloud Director Web Console cannot be used to access resources at a remote association member.

**Important** You must use the vCloud API to associate sites. After two sites have been associated, you can use the vCloud API or the vCloud Director Tenant Portal to associate organizations that occupy those sites. See the *vCloud API Programming Guide for Service Providers* and the *vCloud Director Tenant Portal 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 vCloud Director server group (a group of servers that share a vCloud 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 vCloud Director server group. A system administrator whose authority extends to more than one vCloud Director server group can configure those server groups as an association of vCloud Director sites.

**Associations of Organizations**

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

**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.

With the exception of the System organization, which must use the vCloud Director integrated IDP, association members are free to choose the IDP that works best for them.
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. Note that 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). Unless a site has only a single cell, it must also configure a load balancer that distributes incoming requests across all of 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.

Site Status

After you have created a site association, the system periodically retrieves the status of the remote site and updates that status in the local site’s vCloud Director database. This so-called heartbeat process runs with the identity of the Multisite system user, a local vCloud Director user account created in the System organization during vCloud 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 vCloud API request that retrieves the status of the remote member of a site association.

Create or Update Object Metadata

vCloud Director provides a general-purpose facility for associating user-defined metadata with an object. An administrator or object owner can use the Metadata tab in the object's property page to access an object's metadata.

Object metadata gives service providers and tenants a flexible way to associate user-defined properties (name=value pairs) with objects. Object metadata is preserved when objects are copied, and can be included in vCloud API query filter expressions.

The object owner can create or update metadata for the following types of objects.

- Catalog
- Catalog Item
- Independent Disk
- Media
- Organization VDC Network
- vApp
- vApp Template
- Vm

You must be a system administrator to create or update metadata for the following types of objects.
- Provider VDC
- Provider VDC Storage Profile
- Organization VDC
- VdcStorageProfile

Procedure
1. Open the object's Properties page.
2. Click the Metadata tab.
   - This tab displays any existing metadata and allows you to create new metadata or update existing metadata.
3. (Optional) Create new metadata.
   a. Select a metadata Type from the drop-down control.
   b. Type a Name and a Value for the metadata.
      - The name must be unique within the universe of metadata names attached to this object.
   c. Specify an access level for the new metadata item.
      - If you are a system administrator, this tab allows you to restrict user access to metadata items that you create. You can also choose to hide the metadata item from any user who is not a system administrator.
   d. Click Add to attach the new metadata item to the object.
4. (Optional) Update existing metadata.
   a. Double-click an Existing metadata item.
   b. Modify or delete the item.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Update the item's value. You cannot update the name of a metadata item, but you can delete the existing item and create a new one with a different name.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the item</td>
</tr>
<tr>
<td>Reset</td>
<td>Restore an item you have been editing to its previous value.</td>
</tr>
</tbody>
</table>
Managing vSphere Resources

After you add vSphere resources to the vCloud Director system, you can perform some management functions from vCloud Director. You can also use the vSphere Client to manage these resources.

vSphere resources include vCenter servers, resource pools, ESXi hosts, datastores, and network switches and ports.

This chapter includes the following topics:

- Managing vCenter Servers
- Managing vSphere ESXi Hosts
- Creating and Managing VM-Host Affinity Rules
- Discovering and Adopting vApps
- Managing vSphere Datastores
- Managing Stranded Items
- View Resource Pool Properties
- View Storage Policy Properties

Managing vCenter Servers

After you attach a vCenter Server to vCloud Director, you can modify its settings, reconnect to the vCenter Server, and enable or disable it.

Register vCloud Director with a vCenter Server

You can register vCloud Director with the vCenter Servers it uses.

After you register vCloud Director, it appears as an extension in the vSphere Client Solutions Manager tab. In addition, the vSphere Client sets the Managed By property for vCloud Director-managed virtual machines, which protects those virtual machines from being modified using the vSphere Client.

Procedure

1. Click the Manage & Monitor tab and click vCenters in the left pane.
2. Right-click the vCenter Server name and select Refresh.
3 Click Yes.

Modify vCenter Server Settings

If the connection information for a vCenter Server changes, or if you want to change how its name or description appears in vCloud Director, you can modify its settings.

Procedure

1 Click the Manage & Monitor tab and click vCenters in the left pane.
2 Right-click the vCenter Server name and select Properties.
3 Click the General tab.
4 Type the Host name or IP address and Port Number of the vCenter Server.
5 Type the User name and Password for the vCenter Server.
6 Type a vCenter name. This is the name vCloud Director uses to identify this vCenter Server.
7 (Optional) Type a Description of the vCenter Server.
8 Select the vCloud Web Client URL for vCloud Director to use for Open in vSphere Web Client operations.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use vSphere Services to provide this URL</td>
<td>Select this option if vCloud Director is configured to use vSphere Lookup. vSphere Lookup provides the URL to vCloud Director.</td>
</tr>
<tr>
<td>Use the following URL</td>
<td>Select this option if vCloud Director is not configured to use vSphere Lookup. Type the vSphere Web Client URL for the selected vCenter Server.</td>
</tr>
</tbody>
</table>

9 Click OK.

Reconnect a vCenter Server

If vCloud Director loses it connection to a vCenter Server, or if you change the connection settings, you can try to reconnect.

Procedure

1 Click the Manage & Monitor tab and click vCenters in the left pane.
2 Right-click the vCenter Server name and select Reconnect vCenter.
3 Read the informational message and click Yes to confirm.

Enable or Disable a vCenter Server

You can disable a vCenter Server to perform maintenance.

Procedure

1 Click the Manage & Monitor tab and click vCenters in the left pane.
2 Right-click the vCenter Server name and select **Disable** or **Enable**.

3 Click **Yes**.

### Remove a vCenter Server

You can remove a vCenter Server to stop using its resources with vCloud Director.

**Prerequisites**

Before you can remove a vCenter server, you must disable it and delete all of the provider virtual datacenters that use its resource pools.

**Procedure**

1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.

2 Right-click the vCenter Server name and select **Detach**.

3 Click **Yes**.

### Prepare and Upgrade a vCenter Server Attached to vCloud Director

Before you upgrade a vCenter Server that is attached to vCloud director, you must prepare the server by disabling it in vCloud Director.

Familiarize yourself with the *vSphere Upgrade* documentation.

**Procedure**

1 In the vCloud Director web console, click the **Manage & Monitor** tab and click **vCenters** in the left pane.

2 Right-click the vCenter Server name and select **Disable**.

3 Click **Yes**.

4 Upgrade vCenter Server.

5 In the vCloud Director web console, right-click the vCenter Server name and select **Enable**.

6 Click **Yes**.

7 Right-click the vCenter Server name and select **Refresh** to refresh the vCenter Server system's registration.

### Modify NSX Manager Settings

Modify NSX Manager connection settings if those settings change or you want to connect a different instance of NSX Manager.

**Procedure**

1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.
2 Right-click the vCenter Server name and select Properties.
3 On the NSX Manager tab, type the new settings and click OK.

Managing vSphere ESXi Hosts

You can prepare hosts for use with vCloud Director, enable or disable hosts, upgrade, and repair hosts.

Enable or Disable an ESXi Host

You can disable a host to prevent vApps from starting up on the host. Virtual machines that are already running on the host are not affected.

To perform maintenance on a host, migrate all vApps off of the host or stop all vApps and then disable the host.

Procedure
1 Click the Manage & Monitor tab and click Hosts in the left pane.
2 Right-click the host name and select Enable Host or Disable Host.

vCloud Director enables or disables the host for all provider virtual datacenters that use its resources.

Move Virtual Machines from one ESXi Host to Another

You can move all the virtual machines from one ESXi host to other hosts in the same cluster. Use this procedure when you need to perform maintenance on a host without affecting running virtual machines.

Prerequisites
Disable the host.

Procedure
1 Click the Manage & Monitor tab and click Hosts in the left pane.
2 Right-click the host name and select Redeploy all VMs.
3 Click Yes.

vCloud Director puts the host into maintenance mode and moves all of its virtual machines to other hosts in the same cluster.

Prepare or Unprepare an ESXi Host

After you add an ESXi host to a VMware vSphere® cluster that vCloud Director uses, you must prepare the host before a provider virtual datacenter can use its resources. Unpreparing a host makes it unavailable for use by vCloud Director.

You cannot prepare a host that is in lockdown mode. After you prepare a host, you can enable lockdown mode.
**Prerequisites**

1. Redeploy all VMs on the host to other hosts. See Move Virtual Machines from one ESXi Host to Another.

2. Disable the host.

**Procedure**

1. Click the Manage & Monitor tab and click Hosts in the left pane.

2. Right-click the host name and select Prepare Host or Unprepare Host.

   If you are preparing a host, supply the username and password of a host administrator, then click OK.

**Upgrade an ESXi 5. x Host Agent**

When you prepare an ESXi 5.x host, vCloud Director installs agent software on the host. The agent software is not installed on ESXi 6.x and later. After you upgrade an ESXi 5.x host to a later 5.x release, you must upgrade its host agent.

**Prerequisites**

The host must be running an ESXi 5.x release. If the host is running 6.x or later, the Upgrade Host option is unavailable.

**Procedure**

1. Click the Manage & Monitor tab and click Hosts in the left pane.

2. Right-click the host name and select Upgrade Host.

**Repair an ESXi 5. x Host**

If the vCloud Director agent on an ESXi 5.x host cannot be contacted, try to repair the host.

**Prerequisites**

The host must be running an ESXi 5.x release. If the host is running 6.x or later, the Repair Host option is unavailable.

**Procedure**

1. Click the Manage & Monitor tab and click Hosts in the left pane.

2. Right-click the host name and select Repair Host.

**Creating and Managing VM-Host Affinity Rules**

A vCloud Director system administrator can create groups of VMs in a resource pool, then use VM-Host affinity rules to specify whether members of a VM group should be deployed on members of a vSphere host DRS Group.
vCloud Director VM-Host affinity rules provide vCloud Director system administrators with a way to specify how vSphere Distributed Resource Scheduler (DRS) should place VMs on hosts in a resource pool. VM-Host affinity rules can be useful when host-based licensing requires VMs that are running certain applications to be placed on hosts that are licensed to run those applications. They can also be useful when virtual machines with workload-specific configurations require placement on hosts that have certain characteristics. The technical white paper Best Practices for Performance Tuning of Telco and NFV Workloads in vSphere (http://www.vmware.com/files/pdf/techpaper/vmware-tuning-telco-nfv-workloads-vsphere.pdf) provides several examples of virtual machine configurations that require specific host properties.

**Host Groups and Vm Groups**

A vSphere VM-Host affinity rule is a rule of type Virtual Machines to Hosts, and must specify a host group and a VM group. Before a vCloud Director system administrator can create a VM-Host affinity rule, a vSphere administrator must create at least one host DRS group in a resource pool mapped to a vCloud Director Provider VDC, and a vSphere administrator or vCloud Director system administrator must create a VM group in the same resource pool. VM-Host affinity rules express an affinity in all members of a VM group for all hosts in a host DRS group, so all hosts in a group should share one or more characteristics that a VM can require from a host. For example, you can group hosts on the basis of the application licenses they carry, and group VMs on the basis of the application licenses they require. You can then create VM-Host affinity rules that place VMs on hosts that carry the required licenses.

Because VM-Host affinity rules are properties of a resource pool, all members of groups that are subject to a rule must be deployed in the same resource pool. If a virtual machine or host is removed from the resource pool, the system removes it from any host group or VM group of which it is a member. The system does not update the group when the host or VM is returned to the resource pool.

**Affinity Rule Interactions and Conflicts**

All VM-Host affinity rules in a resource pool have the same precedence. This configuration has implications for how the rules interact. For example, a virtual machine that is a member of two VM groups, each of which is named in a different required VM-Host rule, can run only on hosts that belong to both of those host groups. When you create a VM-Host affinity rule, the system does not check for potential interactions of this kind.

The system does check for conflicts that could arise when applying multiple mandatory rules. For example, if you group VMs and hosts in a way that enables you to create a mandatory anti-affinity rule that applies to a VM and a host that are members of other groups that are subject to a different mandatory affinity rule, the system cannot apply to either rule. When two or more VM-Host affinity rules conflict in this way, the system applies the oldest rule and disables the others. You can correct the problem by making the rules optional, or by grouping the VMs and hosts in ways that minimize the chances of this sort of mandatory rule conflict occurring.
Affinity Rules and vSphere Resource Management

vSphere resource management features such as DRS, vSphere HA, and vSphere DPM never take any action that can violate a mandatory VM-Host affinity rule.

- DRS does not evacuate virtual machines to place a host in maintenance mode.
- DRS does not place virtual machines for power-on or load balance virtual machines.
- vSphere HA does not perform failovers.
- vSphere DPM does not optimize power management by placing hosts into standby mode.

To avoid these situations, be careful when you create more than one mandatory affinity rule that affects a specific VM-host pair. Be sure that the resource pool contains enough hosts so that losing a host does not leave the system with no host on which a VM that is governed by a rule can run. Rules that are not mandatory can be violated to allow the proper functioning of DRS, vSphere HA, and vSphere DPM.

Create or Update a Host Group

A host group is a vSphere host DRS group. A vSphere administrator must create host DRS groups in a resource pool mapped to a vCloud Director Provider VDC before they can be used in vCloud Director VM-Host affinity rules.

vSphere host DRS groups created in resource pools that are mapped to a Provider VDC appear in those resource pools and can be named in VM-Host affinity rules. For more information about host DRS groups, see the VMware vSphere ESXi and vCenter Server Documentation.

Procedure

- Host groups are properties of a resource pool. Select a resource pool from the Resource Pools list under vSphere Properties.
  
  Host DRS groups in the resource pool are listed on its Host Groups tab.

Create or Update a VM Group

A VM group is a collection of virtual machines with similar host requirements. The virtual machines must all be in the same resource pool.

Prerequisites

You must be a system administrator to create or update a VM group.

Procedure

1. VM groups are properties of a resource pool. Select a resource pool from the Resource Pools list under vSphere Properties.

   VM groups in the resource pool are listed on its VM Groups tab. To see a list of all VM groups in all resource pools, click VM Groups under vSphere Properties.
To create a VM group in the resource pool, click the plus sign icon on the VM Groups tab to open the Create VM Group window.

Give the group a name and click OK.

After the system creates the group, you can add VMs to it.

To edit a VM group to add or remove VMs, click VM Groups under vSphere Properties, then right-click the group name in the VM Groups list and select Edit.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add VMs to the group</td>
<td>Select one or more VMs from the upper table and click Add.</td>
</tr>
<tr>
<td>Remove VMs from the group</td>
<td>Select one or more VMs from the lower table and click Remove.</td>
</tr>
</tbody>
</table>

Create or Update a VM-Host Affinity Rule

A VM-Host affinity rule specifies a relationship between a host group and a VM group in the same resource pool. A system administrator can create, enable, disable or delete a VM-Host affinity rule.

After you create a VM-Host affinity rule, you can update it in the following ways:

- Enable the rule.
- Disable the rule.
- Delete the rule.

To make any other change (for example, to change the VM Group or Host Group), you must create a new rule.

vSphere VM-Host affinity rules that are created in resource pools that are mapped to a Provider VDC appear in each pool shown in the Resource Pools list under vSphere Properties. For more information about host DRS VM-Host affinity, see the VMware vSphere ESXi and vCenter Server Documentation.

Prerequisites

- This operation is restricted to system administrators.
- You cannot create VM-Host affinity rule in a resource pool that does not contain at least one host group and one VM group.

Procedure

1. Choose a resource pool to contain the rule.

   Select a resource pool from the Resource Pools list under vSphere Properties. VM-Host affinity rules in the resource pool are listed on its Affinity Rules tab.
2 To create a VM-Host affinity rule in the resource pool, click the plus sign icon on the **Affinity Rules** tab to open the New VM-Host Affinity Rule window.

You must specify a name, VM Group, and Host Group for the rule.

a Type a name for the rule in the **Rule Name** field.

b Select a **VM Group** and a **Host Group** to which the rule applies.

Use the drop-down menus to list all VM groups and host groups in the selected resource pool. If the resource pool does not contain at least one VM group and one host group, you cannot create a rule.

c Specify the polarity of the rule. Click **Must run on hosts** to create an affinity rule. Click **Must not run on hosts** to create an anti-affinity rule.

d Enable or disable the rule.

e Specify whether or not the rule is mandatory.

Mandatory rules are more likely to cause conflicts that can affect system behavior, especially where a VM is the subject of multiple mandatory rules. See **Affinity Rule Interactions and Conflicts**.

3 To enable, disable, or remove an existing VM-Host affinity rule, right-click the rule name on the **Affinity Rules** tab and select one of the available actions.

### Discovering and Adopting vApps

In the default configuration, an organization VDC automatically discovers vCenter VMs that were created in any resource pool that backs the VDC. The system constructs a simplified vApp, owned by the system administrator, to contain each discovered VM. After the system administrator grants you access to a discovered vApp, you can reference the VM in it when you compose or recompose a vApp, or modify the vApp to adopt it and import it.

Discovered vApps contain exactly one VM, and are subject to several constraints that do not apply to vApps created in vCloud Director. Whether or not you adopt them, they can be useful as a source of VMs to use when composing or recomposing a vApp.

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

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

### Enabling VM Discovery

VM discovery is enabled by default. To disable VM discovery, a system administrator must clear the **VM discovery enabled** check box on the **System Settings > General** tab. An organization administrator can use the vCloud API to disable VM discovery for individual VDCs, or for all VDCs in an organization.
Using a VM From a Discovered vApp

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

Adopting a Discovered vApp

To adopt a discovered vApp, modify any of its properties besides name, description, or lease settings. After you have adopted a discovered vApp, the system imports it and treats it as though it was created in vCloud Director. When an adopted vApp is retrieved with a vCloud API request, it includes an element named autoNature. This element has a value of false if the discovered vApp was adopted or was created in vCloud Director. You cannot revert an adopted vApp to a discovered vApp.

If you delete or move the VM that a discovered vApp contains, the system also removes the containing vApp. This behavior does not apply to adopted vApps.

The vApp created to contain a discovered vCenter VM is similar to the one created when you manually import a VM as a vApp, but it is simplified in ways that might require you to modify it before you can deploy it in your VDC. For example, you might have to edit its networking and storage properties, and make other adjustments specific to the needs of your organization.

Managing vSphere Datastores

You can enable or disable vSphere datastores in the vCloud Director system, configure low disk space warnings for datastores, and remove datastores from the vCloud Director system.

Enable or Disable a Datastore

You can enable or disable a datastore that has been added to a provider virtual datacenter. You must disable a datastore before you can remove it from vCloud Director.

When you disable a datastore, you cannot start vApps that are associated with the datastore or create vApps on the datastore.

Procedure

1. Click the Manage & Monitor tab and click Datastores in the left pane.
2. Right-click the datastore name and select Enable or Disable.

vCloud Director enables or disables the datastore for all provider virtual datacenters that use its resources.
Configure Low Disk Space Warnings for a Datastore

You can configure low disk space warnings on a datastore to receive an email from vCloud 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.

Procedure

1. Click the Manage & Monitor tab and click Datastores in the left pane.
2. Right-click the datastore name and select Properties.
3. On the General tab, select the disk space thresholds for the datastore.
   - You can set two thresholds, yellow and red. When vCloud Director sends an email alert, the message indicates which threshold was crossed.
4. Click OK.

vCloud Director sends an email alert when the datastore crosses a threshold.

Enable VAAI for Fast Provisioning on a Datastore

Enable VAAI for fast provisioning to allow offloading of clone operations to compatible NAS arrays.

Important

In-place consolidation of a fast-provisioned VM is not supported on storage containers that employ native snapshots. VVOLs and VAAI-enabled datastores use native snapshots, so fast-provisioned VMs deployed to one of these storage containers cannot be consolidated. If you need to consolidate a fast-provisioned VM deployed to a VVOL or VAAI-enabled datastore, you must relocate it to a different storage container.

Procedure

1. Click the Manage & Monitor tab and click Datastores in the left pane.
2. Right-click the datastore name and select Properties.
3. On the General tab, select Enable VAAI for fast provisioning.
4. Click OK.

Managing Stranded Items

When you delete an object in vCloud Director and that object also exists in vSphere, vCloud Director attempts to delete the object from vSphere. In some situations, vCloud 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

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

**Procedure**

1. Click the **Manage & Monitor** tab and click **Stranded Items** in the left pane.
2. Right-click a stranded item and select **Delete**.
3. Click **Yes**.
   
   vCloud Director attempts to delete the stranded item from vSphere.
4. Refresh the page display.

   If the delete operation is successful, vCloud Director removes the item from the stranded items list.

**What to do next**

If the delete operation is unsuccessful, you can force delete the item. See Force Delete a Stranded Item.

Force Delete a Stranded Item

If vCloud Director cannot delete a stranded item, you can force delete it to remove it from the stranded items list. The stranded item continues to exist in vSphere.

Before you force delete a stranded item, try to delete it. See Delete a Stranded Item.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Stranded Items** in the left pane.
2. Right-click a stranded item and select **Force Delete**.
3. Click **Yes**.

   vCloud Director removes the item from the stranded items list.

View Resource Pool Properties

You can view resource pool properties, such as memory reservation and datastores available to the resource pool.

**Procedure**

1. On the **Manage & Monitor** tab, click **Resource Pools**.
2. Right-click the resource pool and click **Properties**.

   vCloud Director displays the following resource pool properties.
Table 6-1. Resource Pool Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the resource pool.</td>
</tr>
<tr>
<td>Memory reservations (used/total)</td>
<td>The total and used memory reservations for the resource pool, in MB.</td>
</tr>
<tr>
<td>CPU reservations (used/total)</td>
<td>The total and used memory reservations for the resource pool, in MHz.</td>
</tr>
<tr>
<td>Datastore</td>
<td>The name of each datastore available to the resource pool.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of each datastore available to the resource pool.</td>
</tr>
<tr>
<td>Connected</td>
<td>Which of the datastores available to the resource pool are connected. A green check mark indicates a datastore is connected. A red X indicates a datastore is disconnected.</td>
</tr>
<tr>
<td>Capacity (used/ total)</td>
<td>The used and total capacity of each datastore available to the resource pool.</td>
</tr>
<tr>
<td>% Used</td>
<td>The percentage of each datastore that is currently in use.</td>
</tr>
</tbody>
</table>

View Storage Policy Properties

You can view a storage policy's datastores and datastore clusters.

Procedure

2. Right-click the storage policy and click Properties.

vCloud Director displays a list of the storage policy's datastores and datastore clusters.
Managing Organizations

After you create an organization, you can modify its properties, enable or disable it, or delete it.

This chapter includes the following topics:

- Enable or Disable an Organization
- Delete an Organization
- Add a Catalog to an Organization
- Editing Organization Properties
- Managing Organization Resources
- Managing Organization vApps and Virtual Machines
- Migrate Tenant Storage

Enable or Disable an Organization

Disabling an organization prevents users from logging in to the organization and terminates the sessions of currently logged in users. Running vApps in the organization continue to run.

A system administrator can allocate resources, add networks, and so on, even after an organization is disabled.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Enable or Disable.

Delete an Organization

Delete an organization to permanently remove it from vCloud Director.

Prerequisites

Before you can delete an organization, you must disable it and delete all organization virtual datacenters, templates, media files, and vApps in the organization.
Procedure

1. Click the Manage & Monitor tab and click Organization in the left pane.
2. Right-click the organization name and select Delete.
3. Click Yes.

Add a Catalog to an Organization

You can add a catalog to an organization to contain its uploaded and imported vApp templates and media files. An organization can have multiple catalogs and control access to each catalog individually.

Prerequisites
Verify that you have an organization in which to create a catalog.

Procedure

1. Click the Home tab and click Add a catalog to an organization.
2. Select an organization name and click Next.
3. Type a catalog name and optional description and click Next.
4. Select the publishing option and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not publish this catalog to other organizations</td>
<td>The items added to the catalog are only available within the organization.</td>
</tr>
<tr>
<td>Publish to all organizations</td>
<td>The items added to the catalog are available to all of the organizations in the vCloud Director installation. The administrators of each organization can choose which catalog items to provide to their users.</td>
</tr>
</tbody>
</table>

5. Review the catalog settings and click Finish.

Editing Organization Properties

You can edit the properties of an existing organization, including the organization name and description, LDAP options, the catalog publishing policy, email preferences, and storage and processing limits.

- **Modify an Organization Name**
  As your vCloud Director installation grows, you might want to assign a more descriptive name to an existing organization.

- **Modify an Organization Full Name and Description**
  As your vCloud Director installation grows, you might want to assign a more descriptive full name or description to an existing organization.
Modify Organization LDAP Options
You can use an LDAP service to provide a directory of users and groups to import into an organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.

Modify Organization Catalog Sharing, Publishing, and Subscription Policies
Catalogs provide organization users with catalogs of vApp templates and media that they can use to create vApps and install applications on virtual machines. Catalogs can be shared between organizations in different instances of vCloud Director, between organizations in the same instance of vCloud Director, or remain accessible only within the host organization.

Modify Organization Email Preferences
vCloud Director requires an SMTP server to send user notification and system alert emails. You can modify the settings you specified when you created the organization.

Modify Organization Lease, Quota, and Limit Settings
Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. You can modify these settings to prevent users from depleting or monopolizing an organization's resources.

Modify an Organization Name
As your vCloud Director installation grows, you might want to assign a more descriptive name to an existing organization.

Prerequisites
You must disable the organization before you can rename it.

Procedure
1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Properties.
3. On the General tab, type a new organization name and click OK.
The internal organization URL changes to reflect the new name.

Modify an Organization Full Name and Description
As your vCloud Director installation grows, you might want to assign a more descriptive full name or description to an existing organization.

Procedure
1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Properties.
3. On the General tab, type a new full name or description and click OK.
Modify Organization LDAP Options

You can use an LDAP service to provide a directory of users and groups to import into an organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.

For more information about entering custom LDAP settings, see Configuring System LDAP Settings.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Properties.
3. Click the LDAP Options tab.
4. Select the new source for organization users.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Organization administrator creates a local user account for each user in the organization. You cannot create groups if you select this option.</td>
</tr>
<tr>
<td>VCD system LDAP service</td>
<td>Use the LDAP service for the vCloud Director system as the source for organization users and groups.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Connect the organization to its own private LDAP service.</td>
</tr>
</tbody>
</table>

5. Provide any additional information required by your selection.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Click OK.</td>
</tr>
<tr>
<td>VCD system LDAP service</td>
<td>(Optional) Type the distinguished name of the organizational unit (OU) to use to limit the users that you can import into the organization and click OK. If you do not enter anything, you can import all users in the system LDAP service into the organization.</td>
</tr>
<tr>
<td>Note</td>
<td>Specifying an OU does not limit the LDAP groups you can import. You can import any LDAP group from the system LDAP root. However, only users who are in both the OU and the imported group can log in to the organization.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Click the Custom LDAP tab, type the custom LDAP settings for the organization, and click OK.</td>
</tr>
</tbody>
</table>

System administrators and organization administrators who are currently logged in cannot import users and groups using the modified LDAP options until the cache for their current session expires or they log out and log in again.
Modify Organization Catalog Sharing, Publishing, and Subscription Policies

Catalogs provide organization users with catalogs of vApp templates and media that they can use to create vApps and install applications on virtual machines. Catalogs can be shared between organizations in different instances of vCloud Director, between organizations in the same instance of vCloud Director, or remain accessible only within the host organization.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Properties.
3. Click the Catalog tab.
4. Select a catalog publishing option and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot publish catalogs</td>
<td>Organization administrator cannot publish any catalogs for users outside of the organization.</td>
</tr>
<tr>
<td>Allow publishing catalogs to all organizations</td>
<td>Organization administrator can publish a catalog for users in all organizations.</td>
</tr>
</tbody>
</table>

5. Set the organization catalog policies.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow sharing catalogs to other organizations</td>
<td>Allows organization administrators to share this organization's catalogs with other organizations in this instance of vCloud Director. If you do not select this option, organization administrators are still able to share catalogs within the organization.</td>
</tr>
<tr>
<td>Allow creation of catalog feeds for consumption by external organizations</td>
<td>Allows organization administrators to share this organization's catalogs with organizations outside this instance of vCloud Director.</td>
</tr>
<tr>
<td>Allow subscription to external catalog feeds</td>
<td>Allows organization administrators to subscribe this organization to catalog feeds from outside this instance of vCloud Director.</td>
</tr>
</tbody>
</table>

6. Click OK.

Modify Organization Email Preferences

vCloud Director requires an SMTP server to send user notification and system alert emails. You can modify the settings you specified when you created the organization.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Properties.
3. Click the Email Preferences tab.
4 Select an SMTP server option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default SMTP server</td>
<td>Organization uses the system SMTP server.</td>
</tr>
<tr>
<td>Set organization SMTP server</td>
<td>Organization uses its own SMTP server. If you select this option, type the</td>
</tr>
<tr>
<td></td>
<td>DNS host name or IP address and port number of the SMTP server. (Optional)</td>
</tr>
<tr>
<td></td>
<td>Select the Requires authentication check box and type a user name and password.</td>
</tr>
</tbody>
</table>

5 Select a notification settings option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default notification</td>
<td>Organization uses the system notification settings.</td>
</tr>
<tr>
<td>settings</td>
<td></td>
</tr>
<tr>
<td>Set organization notification</td>
<td>Organization uses its own notification settings. If you select this option,</td>
</tr>
<tr>
<td>settings</td>
<td>type an email address that appears as the sender for organization emails,</td>
</tr>
<tr>
<td></td>
<td>type text to use as the subject prefix for organization emails, and select</td>
</tr>
<tr>
<td></td>
<td>the recipients for organization emails.</td>
</tr>
</tbody>
</table>

6 (Optional) Type a destination email address and click Test Email Settings to verify that all SMTP server settings are configured as expected.

7 Click OK.

Modify Organization Lease, Quota, and Limit Settings

Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. You can modify these settings to prevent users from depleting or monopolizing an organization's resources.

For more information about leases, see Understanding 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. You can also specify what happens to vApps and vApp templates when their storage lease expires.

Quotas determine how many virtual machines each user in the organization can store and power on in the organization's virtual datacenters. The quota you specify acts as a default for all new users added to the organization.

Certain vCloud Director operations, for example copy and move, are more resource intensive than others. Limits prevent resource-intensive operations from affecting all the users in an organization and also provide a defense against denial-of-service attacks.

Procedure

1 Click the Manage & Monitor tab and click Organizations in the left pane.

2 Right-click the organization name and select Properties.

3 Click the Policies tab.

4 Select the lease options for vApps and vApp templates.
5 Select the quotas for running and stored virtual machines.

Quotas set at the user level supersede quotas set at the organization level.

6 Choose the maximum system limits for resource intensive operations, console connections to a virtual machine, and data centers per organization.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of resource intensive operations per user</td>
<td>Type the maximum number of simultaneous resource intensive operations per user, or select Inherit System Limit.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per user</td>
<td>Type the maximum number of queued resource intensive operations per user, or select Inherit System Limit.</td>
</tr>
<tr>
<td>Number of resource intensive operations per organization</td>
<td>Type the maximum number of simultaneous resource intensive operations per organization, or select Inherit System Limit.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per organization</td>
<td>Type the maximum number of queued resource intensive operations per organization, or select Inherit System Limit.</td>
</tr>
<tr>
<td>Number of simultaneous connections per VM</td>
<td>Type the maximum number of simultaneous console connections per virtual machine, or select Inherit System Limit.</td>
</tr>
<tr>
<td>Number of virtual data centers per organization</td>
<td>Type the maximum number of organization virtual data centers per organization, or select Inherit System Quota.</td>
</tr>
</tbody>
</table>

These limits provide a defense against denial of service attacks.

7 Click OK.

Managing Organization Resources

vCloud Director organizations obtain their resources for one or more organization virtual datacenters. If an organization needs more resources, you can add a new organization virtual datacenter or modify an existing organization virtual datacenter. You can take resources away from an organization by removing or modifying an organization virtual datacenter.

For more information about adding an organization virtual datacenter, see Create an Organization Virtual Datacenter.

For information about removing an organization virtual datacenter, see Delete an Organization Virtual Datacenter.

For information about modifying the resources available to an existing organization virtual datacenter, see Edit Organization Virtual Datacenter Allocation Model Settings, and Edit Organization Virtual Datacenter Storage Settings.
Managing Organization vApps and Virtual Machines

Some tasks related to managing organization vApps and virtual machines can only be performed by a system administrator. For example, system administrators can add vSphere virtual machines to an existing vApp, create a vApp based on a vSphere virtual machine, and place a vApp in maintenance mode.

For more information about working with vApps in an organization, see the VMware vCloud Director User's Guide.

Add a vSphere Virtual Machine to a vApp

A system administrator can import a vSphere virtual machine into an existing vCloud Director vApp.

Prerequisites

You must be logged in to vCloud Director as a system administrator and the organization containing the vApp must have an available organization virtual datacenter.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3. Click the My Cloud tab and click vApps in the left pane.
4. Right-click the vApp name and select Open.
5. On the Virtual Machines tab, click the Actions button and select Import from vSphere.
6. Select a vCenter Server and a virtual machine.
7. Type a name and optional description for the virtual machine.
8. Select whether to copy or move the source virtual machine.
9. Click OK.

Create a vApp Based on a vSphere Virtual Machine

A system administrator can import a vSphere virtual machine to an organization as a vCloud Director vApp.

Prerequisites

Verify that you are logged in to vCloud Director as a system administrator and that the organization has an available organization virtual datacenter.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3 Click the My Cloud tab and click vApps in the left pane.

4 Click Import from vSphere.

5 Select a vCenter Server and a virtual machine.

6 Type a name and optional description for the vApp and select a destination organization virtual datacenter.

7 Select whether to copy or move the source virtual machine.

8 Click OK.

**Place a vApp in Maintenance Mode**

A system administrator can place a vApp in maintenance mode to prevent non-administrator users from changing the state of the vApp. This is useful, for example, when you want to back up a vApp using a third-party backup solution.

When a vApp is in maintenance mode, non-system administrator users cannot perform any actions that modify the state of the vApp or its virtual machine. They can view information about the vApp and its virtual machines and access the virtual machine consoles.

Placing a vApp in maintenance mode does not affect any currently running tasks that involve the vApp.

**Prerequisites**

You must be logged in to vCloud Director as a system administrator.

**Procedure**

1 Click the Manage & Monitor tab and click Organizations in the left pane.

2 Right-click the organization name and select Open.

3 Click the My Cloud tab and click vApps in the left pane.

4 Right-click the vApp name and select Enter Maintenance Mode.

5 Click Yes.

The status of the vApp changes to In Maintenance Mode. The vApp remains in maintenance mode until you select Exit Maintenance Mode.

**Force Stop a Running vApp**

A system administrator can force stop a running vApp when an organization user is unable to do so.

In some cases, a user may be unable to stop a running vApp. If traditional methods for stopping the vApp fail, you can force stop the vApp to prevent the user from getting billed.

Force stopping a vApp does not prevent the vApp from consuming resources in vSphere. After you force stop a vApp in vCloud Director, use the vSphere Client to check the status of the vApp in vSphere and take the necessary action.
Prerequisites

You must be logged in to vCloud Director as a system administrator.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3. Click the My Cloud tab and click vApps in the left pane.
4. Right-click the running vApp and select Force Stop.
5. Click Yes.

Fast Provisioning of Virtual Machines

Fast provisioning saves time by using linked clones for virtual machine provisioning operations. Fast provisioning is enabled by default on organization VDCs.

A linked clone is a duplicate of a virtual machine that uses the same base disk as the original, with a chain of delta disks to track the differences between the original and the clone. If fast provisioning is disabled, all provisioning operations result in full clones.

A linked clone cannot exist on a different vCenter datacenter or datastore than the original virtual machine. vCloud Director creates shadow virtual machines to support linked clone creation across vCenter datacenters and datastores for virtual machines associated with a vApp template. A shadow virtual machine is an exact copy of the original virtual machine. The shadow virtual machine is created on the datacenter and datastore where the linked clone is created. You can view a list of shadow virtual machines associated with a template virtual machine. See View Shadow Virtual Machines Associated With a vApp Template.

Important  In-place consolidation of a fast-provisioned VM is not supported on storage containers that employ native snapshots. VVOLs and VAAI-enabled datastores use native snapshots, so fast-provisioned VMs deployed to one of these storage containers cannot be consolidated. If you need to consolidate a fast-provisioned VM deployed to a VVOL or VAAI-enabled datastore, you must relocate it to a different storage container.

View Shadow Virtual Machines Associated With a vApp Template

Shadow virtual machines support linked clones of virtual machines that are associated with vApp templates across vCenter datacenters and datastores.

A shadow virtual machine is an exact copy of the original virtual machine that vCloud Director creates on the datacenter and datastore where a linked clone is created. See Fast Provisioning of Virtual Machines.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3 Click **Catalogs**.

4 On the **vApp Templates** tab, double-click the vApp template to open it.

5 Click the **Shadow VMs** tab.

vCloud Director shows a list of shadow virtual machines associated with the vApp template. This list includes the name in vCenter of each shadow virtual machine, the datastore that each shadow virtual machine exists on, and the vCenter server that the shadow virtual machine belongs to.

**Migrate Tenant Storage**

A system administrator can migrate all of a tenant organization's vApps, independent disks, and catalog items to another datastore.

Before you decommission a datastore that backs a storage profile used by an organization VDC, you must migrate all the items stored on that datastore to new storage. Even if you're not decommissioning a datastore, you might need to migrate an organization to new storage to take advantage of additional storage capacity or newer storage technologies such as VMware vSAN. The vCloud Director storage migration wizard allows you to select one or more organisations and migrate their stored items from a source datastore to a destination datastore. Before you can migrate organization storage, you'll need to know which datastores the organization is using, and you'll need to create one or more datastores to serve as the destination.

**Important** Tenant storage migration is a resource-intensive operation that can run for a long time, especially when there are many assets to migrate. See VMware Knowledge Base article [https://kb.vmware.com/kb/2151086](https://kb.vmware.com/kb/2151086) for information that can help you plan and execute an effective storage migration.

**Prerequisites**

- This operation is restricted to system administrators and custom roles that have been granted the **Organization: Migrate Tenant Storage** right.
- At least one target datastore must be accessible to the ESXi host running the migrated VM.
- Because migrating a vApp or catalog item must not change its storage profile, one or more of the destination datastores must be associated with each storage profile that's available in the organization VDCs backed by the source datastores.

**Procedure**

1 Launch the wizard.

There are two ways to launch the wizard, which follows the same workflow regardless of how you launch it.

- Click the **Manage & Monitor** tab and click **Organizations** in the left pane. Right-click an organization name and select **Migrate Tenant Storage**.
- Click the **Manage & Monitor** tab and click **Datastores & Datastore Clusters** in the left pane. Right-click a datastore or cluster name and select **Migrate Tenant Storage**.
2 Select one or more organizations to migrate and click Add.
   Click Next to save your choices and continue.

3 Select one or more source datastores and click Add.
   The wizard lists all datastores in the system. You can discover which of these datastores an organization is using by going to each of the organization's VDCs and listing the storage profiles they offer. Open each storage profile in the vSphere Web Client to see the datastores that are part of the storage profile. Select those datastores and click Add to add them to the set of source datastores for this migration.
   Click Next to save your choices and continue.

4 Select one or more destination datastores and click Add.
   You can create destination datastores or use existing ones. At least one destination datastore must be associated with each storage profile that's available in the organization VDCs backed by the source datastores.
   Click Next to save your choices and continue.

5 Review your selections and click Finish to begin the migration.
   You can use the Tenant Migration tab on the Logs page to monitor and cancel tenant storage migrations. See View Ongoing and Completed Tenant Storage Migrations.
Managing System Administrators and Roles

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

This chapter includes the following topics:
- Add a System Administrator
- Import a System Administrator
- Enable or Disable a System Administrator
- Delete a System Administrator
- Edit System Administrator Profile and Contact Information
- Send an Email Notification to Users
- Delete a System Administrator Who Lost Access to the System
- Import a Group
- Delete an LDAP Group
- View Group Properties
- Working With Roles and Rights

Add a System Administrator

You can add a system administrator to vCloud Director by creating a system administrator account. System administrators have full rights to vCloud Director and all of its organizations.

Procedure

1. Click the Administration tab and click Users in the left pane.
2. Click New.
3. Type the account information for the new user and click OK.
Import a System Administrator

To add a user with system administrator rights, you can import an LDAP user or vCenter Single Sign On user as a system administrator. System administrators have full rights to vCloud Director and all of its organizations.

**Prerequisites**

Verify that you have a valid connection to an LDAP server or have vCenter Single Sign On enabled. See Configure vCloud Director to use the vSphere SSO SAML provider.

**Procedure**

1. Click the **Administration** tab and click **Users** in the left pane.
2. Click **Import Users**.
3. Select a **Source** to import users from.
   - **LDAP**: Import users from an LDAP server. Type a full or partial name in the text box and click **Search Users**. Select the users to import and click **Add**.
   - **vSphere SSO**: Import users from vCenter Single Sign On. Type the user names of the users to import and click **Add**. Imported user names must include domain names (ex. user@domain.com). Separate multiple users with carriage returns.
4. Click **OK**.

Enable or Disable a System Administrator

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

**Procedure**

1. Click the **Administration** tab and click **Users** in the left pane.
2. Right-click the user name and select **Enable Account** or **Disable Account**.

Delete a System Administrator

You can remove a system administrator from the vCloud Director system by deleting their account.

**Prerequisites**

Disable the system administrator account.
Procedure
1. Click the Administration tab and click Users in the left pane.
2. Right-click the user name and select Delete.
3. Click Yes.

Edit System Administrator Profile and Contact Information
You can change the password and contact information for a system administrator account. You can only edit account information for local users.

Procedure
1. Click the Administration tab and click Users in the left pane.
2. Right-click the user name and select Properties.
3. Type the new information for the user account and click OK.

Send an Email Notification to Users
You can send an email notification to all users in the entire installation, all system administrators, or all organization administrators. You can send an email notification to notify users about upcoming system maintenance, for example.

Prerequisites
Verify that you have a valid connection to an SMTP server.

Procedure
1. Click the Administration tab and click Users in the left pane.
2. Click Notify.
3. Select the recipients.
4. Type the email subject and message and click Send Email.

Delete a System Administrator Who Lost Access to the System
You can view a list of user accounts that lost access to the system when their LDAP group was deleted from vCloud Director. You can decide whether or not to add the user back into the system and then delete the user from the Lost & Found.

To add a user that was mistakenly removed from the system when their LDAP group was deleted, see Add a System Administrator and Import a System Administrator.
Procedure

1. Click the Administration tab and click Lost & Found in the left pane.
2. Right-click the user name and select Delete User.

Import a Group

To add a group of users with system administrator rights, you can import an LDAP group or a vCenter Single Sign On group as system administrators. System administrators have full rights to vCloud Director and all of its organizations.

Prerequisites

Verify that you have a valid connection to an LDAP server or have vCenter Single Sign On enabled. See Configure vCloud Director to use the vSphere SSO SAML provider.

Procedure

1. Click the Administration tab and click Groups in the left pane.
2. Click Import Groups.
3. Choose a Source to import from.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Import groups from an LDAP server.</td>
</tr>
<tr>
<td></td>
<td>a. Type a full or partial name in the text box and click Search Groups.</td>
</tr>
<tr>
<td></td>
<td>b. Select the groups to import and click Add.</td>
</tr>
<tr>
<td>vSphere SSO</td>
<td>Import groups from vCenter Single Sign On. Type the group name or names and</td>
</tr>
<tr>
<td></td>
<td>click Add. Separate multiple groups with carriage returns.</td>
</tr>
</tbody>
</table>

4. Click OK.

Delete an LDAP Group

You can remove a group of system administrators from the vCloud Director system by deleting their LDAP group.

When you delete an LDAP group, users who have a vCloud Director account based solely on their membership in that group are stranded and cannot log in. See Delete a System Administrator Who Lost Access to the System.

Procedure

1. Click the Administration tab and click Groups in the left pane.
2. Right-click the group name and select Delete.
3. Click Yes to confirm the deletion.
View Group Properties

You can view group properties, such as the name, role, and organization of a group.

Procedure

1. Click the **Administration** tab and click **Groups** in the left pane.
2. Right-click the group name and select **Properties**.

The properties of the group are displayed.

Working With Roles and Rights

A role associates a role name with a set of rights. A newly created organization includes a set of predefined roles and rights inherited from the system. A system administrator can use the vCloud Director Web Console or the vCloud API to create or update role objects in any organization in the system. Organization administrators can use the vCloud API to create or update role objects in organizations they administer.

vCloud 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 **vCloud Director Administrator's Guide**, **vCloud Director User's Guide**, and **vCloud API Programming Guide for Service Providers** 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.

When you create or import a user or import a group, you must assign it a role.

Roles and Rights in an Organization

In previous releases of vCloud Director, roles were global objects created by system administrators and available to all organizations. Beginning with vCloud Director 8.20, role objects are created and managed at the organization level. Each organization is created with a set of predefined roles and the rights contained by those roles. A system administrator can use the vCloud API to grant additional rights to an organization during creation or afterward. A system administrator can also remove rights from an organization. A system administrator can edit a predefined role to add or remove rights.

**Note** When you upgrade vCloud Director from a release earlier than 8.20, all roles that exist in the system, including roles created by system administrators, are treated as predefined roles. Copies of these roles, along with the rights they contain, are propagated to all organizations in the system. Only a system administrator can delete or modify a predefined role.

Related Videos

[Role-Based Access Control in vCloud Director](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vcd_rolebased_access)
Predefined Roles and Their Rights
Each vCloud Director predefined role contains a default set of rights required to perform operations included in common workflows. With the exception of the System Administrator role, each predefined role exists in every organization in the system.

Create, Update, or Delete a Role
A system administrator can use the vCloud Director Web Console or the vCloud API to create or update role objects in any organization in the system. Organization administrators can use the vCloud API to create or update role objects in the organizations they administer.

Copy a Role
A system administrator can use the vCloud Director Web Console to copy a role object within an organization.

Predefined Roles and Their Rights
Each vCloud Director predefined role contains a default set of rights required to perform operations included in common workflows. With the exception of the System Administrator role, each predefined role exists in every organization in the system.

The System Administrator Role
The system administrator role exists only in the System organization. The System organization and system administrator role include all rights. System administrator credentials are established during installation and configuration. A system administrator can create additional system administrator accounts. All system administrators are members of the System organization.

You cannot modify the rights associated with the System Administrator role. A system administrator can use the vCloud Director Web Console or the vCloud API to create or update other role objects in any organization in the system.

Predefined Roles
Predefined roles and the rights they contain are available in all organizations.

<table>
<thead>
<tr>
<th>Role</th>
<th>Rights Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Administrator</td>
<td>After creating an organization, a system administrator can assign the role of organization administrator to any user in the organization. A user with the predefined Organization Administrator role can use the vCloud Director Web Console or the vCloud API to manage users and groups in their organization and assign them roles, including the predefined Organization Administrator role. An organization administrator can use the vCloud API to create or update role objects that are local to the organization. Roles created or modified by an organization administrator are not visible to other organizations.</td>
</tr>
<tr>
<td>Catalog Author</td>
<td>The rights associated with the predefined Catalog Author role allow a user to create and publish catalogs.</td>
</tr>
</tbody>
</table>
vApp Author
The rights associated with the predefined vApp Author role allow a user to use catalogs and create vApps.

vApp User
The rights associated with the predefined vApp User role allow a user to use existing vApps.

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

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

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

With the exception of 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 Roles
A system administrator can use the vCloud Director Web Console to view the list of rights included in a role.

1. Click the Administration tab.
2. Click Roles in the left pane.
3. Right-click a role and select Properties.

An organization administrator can use the vCloud API to view the rights in a role or create new roles local to the organization.
Rights Included in Multiple Predefined Roles

A number of rights are common to many predefined roles. These rights are granted by default to all new organizations, and are available for use in other roles created by the organization administrator.

Table 8-1. Rights Included in Multiple Predefined Roles

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
<th>Organization Administator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp Use Only</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog: Add vApp from My Cloud</td>
<td>Permission to add a vApp from My Cloud to a catalog in my organization.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: CLSP Publish Subscribe</td>
<td>Permission to publish catalogs for external consumption and to subscribe to external catalog feeds. Organization must be configured to allow publishing externally, subscribing to external catalogs, or both.</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Create / Delete a Catalog</td>
<td>Permission to create and delete catalogs.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Edit Properties</td>
<td>Permission to edit catalog properties.</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Publish</td>
<td>Permission to share catalogs with users and groups in other organizations. Organization must be configured to allow sharing catalogs with other organizations.</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Sharing</td>
<td>Permission to share catalogs to users and groups in the same organization.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View ACL</td>
<td>Permission to view the access control list of any catalog in the organization.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View Private and Shared Catalogs</td>
<td>Permission to view both private and shared catalogs in the organization.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: Create</td>
<td>Permission to create independent disks.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: Delete</td>
<td>Permission to delete independent disks.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: Edit Properties</td>
<td>Permission to edit the properties of an independent disk.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: View Properties</td>
<td>Permission to view the properties of an independent disk.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Organization vDC: View</td>
<td>Permission to view all VDCs in the organization.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization vDC: VM-VM Affinity Edit</td>
<td>Permission to edit VM-VM affinity for VMs in all VDCs in the organization.</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: View</td>
<td>Permission to view organization contents.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-1. Rights Included in Multiple Predefined Roles (Continued)

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Template / Media: Copy</td>
<td>Permission to copy or move catalog items (vApp templates or media).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp Template / Media: Create / Upload</td>
<td>Permission to create or upload catalog items (vApp templates or media).</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp Template / Media: Edit</td>
<td>Permission to modify catalog items (vApp templates or media).</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp Template / Media: View</td>
<td>Permission to view catalog items (vApp templates or media).</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp Template: Checkout</td>
<td>Permission to use a vApp template to create a vApp in My Cloud.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp Template: Download</td>
<td>Permission to download a vApp template as an OVF package.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Change Owner</td>
<td>Permission to change the owner of a vApp.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Copy</td>
<td>Permission to make a copy of a vApp.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Create / Reconfigure</td>
<td>Permission to create and reconfigure vApps.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Delete</td>
<td>Permission to delete a vApp.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Download</td>
<td>Permission to download a vApp as an OVF package.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit Properties</td>
<td>Permission to edit vApp general properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit VM CPU</td>
<td>Permission to edit vApp CPU properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Hard Disk</td>
<td>Permission to edit vApp hard disk properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Memory</td>
<td>Permission to edit vApp memory properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit VM Network</td>
<td>Permission to edit vApp network properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit VM Properties</td>
<td>Permission to edit VM general properties.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Manage VM Password Settings</td>
<td>Permission to modify VM passwords.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Power Operations</td>
<td>Permission to change VM power state.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: Sharing</td>
<td>Permission to share a vApp with other members of the organization.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Table 8-1. Rights Included in Multiple Predefined Roles (Continued)

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>vApp Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp: Snapshot Operations</td>
<td>Permission to create, delete, and revert to a vApp snapshot.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Upload</td>
<td>Permission to upload an OVF package as a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Use Console</td>
<td>Permission to open a console connection to a VM in a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: View ACL</td>
<td>Permission to view the access control list of a vApp.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>vApp: View VM metrics</td>
<td>Permission to view current metrics of VMs in a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: VM Boot Options</td>
<td>Permission to edit vApp boot options such as boot delay and recustomization.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Allow metadata mapping domain to vCenter</td>
<td>Permission to create or update vApp object metadata in the VCENTER domain</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCD Extension: View Tenant Portal Plugin Information</td>
<td>Permission to view plug-ins available for the vCloud Director Tenant Portal</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Additional Rights Included in the Predefined Organization Administrator Role

The following additional rights are included in the predefined organization administrator role. They are not included in any other predefined role except system administrator. These rights are granted by default to all new organizations, and are available for use in other roles created by the organization administrator.

Table 8-2. Additional Rights Included in the Predefined Organization Administrator Role

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access All Organization VDCs</td>
<td>Permission to view and modify all VDCs in the organization.</td>
</tr>
<tr>
<td>Catalog: Change Owner</td>
<td>Permission to change to owner of any catalog in the organization.</td>
</tr>
<tr>
<td>Catalog: View Published Catalogs</td>
<td>Permission to view catalogs shared from other organizations.</td>
</tr>
<tr>
<td>Disk: Change Owner</td>
<td>Permission to change the owner of an independent disk.</td>
</tr>
<tr>
<td>General: Administrator Control</td>
<td>Permission to modify objects in the organization.</td>
</tr>
<tr>
<td>General: Administrator View</td>
<td>Permission to view objects in the organization.</td>
</tr>
<tr>
<td>General: Send Notification</td>
<td>Permission to configure notifications sent to members of the organization.  See Configure System Notification Settings.</td>
</tr>
<tr>
<td>Group / User: View</td>
<td>Permission to view local users and groups.</td>
</tr>
</tbody>
</table>
### Table 8-2. Additional Rights Included in the Predefined Organization Administrator Role (Continued)

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid Cloud Operations: Acquire control ticket</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Acquire from-the-cloud tunnel ticket</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Acquire to-the-cloud tunnel ticket</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Create from-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Create to-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Delete from-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Delete to-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: Update from-the-cloud tunnel endpoint tag</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: View from-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations: View to-the-cloud tunnel</td>
<td>This right is required by certain vCloud Director hybrid extensions.</td>
</tr>
<tr>
<td>Organization Network: Edit Properties</td>
<td>Permission to modify properties of an organization VDC network.</td>
</tr>
<tr>
<td>Organization Network: View</td>
<td>Permission to view properties of an organization VDC network.</td>
</tr>
<tr>
<td>Organization vDC Distributed Firewall: Configure Rules</td>
<td>Advanced networking right. See &quot;Manage Distributed Firewall Rules Using the Tenant Portal&quot; in the vCloud Director Tenant Portal Guide.</td>
</tr>
<tr>
<td>Organization vDC Distributed Firewall: View Rules</td>
<td>Advanced networking right. See &quot;Manage Distributed Firewall Rules Using the Tenant Portal&quot; in the vCloud Director Tenant Portal Guide.</td>
</tr>
<tr>
<td>Organization vDC Gateway: Configure Firewall</td>
<td>Advanced networking right. See &quot;Firewall Configuration Using the Tenant Portal&quot; in the vCloud Director Tenant Portal Guide.</td>
</tr>
</tbody>
</table>
### Table 8-2. Additional Rights Included in the Predefined Organization Administrator Role (Continued)

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization vDC Gateway: Convert to Advanced Networking</td>
<td>Permission to convert an Edge Gateway to Advanced Networking.</td>
</tr>
<tr>
<td>Organization vDC Network: View Properties</td>
<td>Permission to view the properties of an organization VDC network. See Configuring Organization Virtual Datacenter Network Services.</td>
</tr>
<tr>
<td>Organization vDC Storage Profile: Set Default</td>
<td>Permission to change the default storage profile for an organization VDC. See Add a VM Storage Policy to a Provider Virtual Data Center.</td>
</tr>
<tr>
<td>Organization vDC: Edit</td>
<td>Permission to change the configuration of an organization VDC.</td>
</tr>
<tr>
<td>Organization vDC: Edit ACL</td>
<td>Permission to create or update VDC access controls. (API only.)</td>
</tr>
<tr>
<td>Organization vDC: Manage Firewall</td>
<td>Permission to manage firewall rules on an Edge Gateway that is not an advanced gateway.</td>
</tr>
<tr>
<td>Organization vDC: View ACL</td>
<td>Permission to view VDC access controls. (API only.)</td>
</tr>
<tr>
<td>Organization: Edit Association Settings</td>
<td>Permission to create or modify an association with another organization. See Configuring and Managing Multisite Deployments.</td>
</tr>
<tr>
<td>Organization: Edit Federation Settings</td>
<td>Permission to modify organization federation (IDP) settings.</td>
</tr>
<tr>
<td>Organization: Edit Leases Policy</td>
<td>Permission to modify default storage and runtime leases for vApps. See Modify Organization Lease, Quota, and Limit Settings.</td>
</tr>
<tr>
<td>Organization: Edit OAuth Settings</td>
<td>Permission to create or modify organization OAuth IDP settings.</td>
</tr>
<tr>
<td>Organization: Edit Password Policy</td>
<td>Permission to create or modify organization password policies.</td>
</tr>
<tr>
<td>Organization: Edit Properties</td>
<td>Permission to modify organization properties. See Editing Organization Properties.</td>
</tr>
<tr>
<td>Organization: Edit Quotas Policy</td>
<td>Permission to modify organization quotas for VMs. See Modify Organization Lease, Quota, and Limit Settings.</td>
</tr>
</tbody>
</table>
Table 8-2. Additional Rights Included in the Predefined Organization Administrator Role (Continued)

<table>
<thead>
<tr>
<th>Right Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization: Edit SMTP Settings</td>
<td>Permission to modify organization SMTP (e-mail) policies. See Configure SMTP Settings.</td>
</tr>
<tr>
<td>Organization: Import User/Group from IdP while Editing VDC ACL</td>
<td>Unused by vCloud Director</td>
</tr>
<tr>
<td>Role: Create, Edit, Delete, or Copy</td>
<td>Permission to create or modify roles in your organization. Permission to change the default storage profile for an organization VDC. See Create, Update, or Delete a Role.</td>
</tr>
<tr>
<td>VDC Template: Instantiate</td>
<td>Permission to create an organization VDC from a template. See Instantiate an Organization Virtual Data Center Template.</td>
</tr>
<tr>
<td>VDC Template: View</td>
<td>Permission to view an organization VDC template. See Instantiate an Organization Virtual Data Center Template.</td>
</tr>
</tbody>
</table>

Create, Update, or Delete a Role

A system administrator can use the vCloud Director Web Console or the vCloud API to create or update role objects in any organization in the system. Organization administrators can use the vCloud API to create or update role objects in the organizations they administer.

Prerequisites

Only a system administrator can use the vCloud Director Web Console create or update role objects.

Procedure

- Click the Administration tab and click Roles in the left pane.
  
The system displays a list of all roles and the organizations in which they exist.

- To create a role, click New.
  
  a Select an organization in which to create the role.
  
  b Type a name and optional description for the role.
  
  c Select the rights for the role.
    
      Expand a right category to see the individual rights it contains. All right categories are displayed by default. To limit the list of right categories displayed to those in which you have selected at least one right to add to the role, select Show only selected rights.
    
  d Click OK to save your changes.
To update a role, right-click an entry in the list (a role and an organization) and select **Properties**.

a. Select the rights for the role.

   Expand a right category to see the individual rights it contains. All right categories are displayed by default. To limit the list of right categories displayed to those in which you have selected at least one right to add to the role, select **Show only selected rights**.

b. Click **OK** to save your changes.

To delete a role, right-click an entry in the list (a role and an organization) and select **Delete**.

Click **Yes** to confirm the deletion.

**Copy a Role**

A system administrator can use the vCloud Director Web Console to copy a role object within an organization.

**Prerequisites**

Only a system administrator can use the vCloud Director Web Console create or update role objects.

**Procedure**

1. Click the **Administration** tab and click **Roles** in the left pane.

   The system displays a list of all roles and the organizations in which they exist.

2. Right-click an entry in the list and select **Copy to**.

   **Important** Regardless of the organization you select in the **Copy Role** dialog, the copy is always created in the source organization.

3. Type a name and optional description for the copied role.

4. Select the rights for the role and click **OK**.

   Expand a right category to see the individual rights it contains. All right categories are displayed by default. To limit the list of right categories displayed to those in which you have selected at least one right to add to the role, select **Show only selected rights**.

A copy of the role is created within the organization.
Managing System Settings

A vCloud Director system administrator can control system-wide settings related to LDAP, email notification, licensing, and general system preferences.

This chapter includes the following topics:

- Modify General System Settings
- General System Settings
- Editing System Email Settings
- Configuring Blocking Tasks and Notifications
- Configuring System LDAP Settings
- Customize the vCloud Director Client UI
- Configuring Public Addresses
- Configure System Limits
- Configure the Account Lockout Policy
- Configure vCloud Director to use the vSphere SSO SAML provider

Modify General System Settings

vCloud Director includes general system settings related to login policy, session timeouts, and so on. The default settings are appropriate for many environments, but you can modify the settings to meet your needs.

For more information, see General System Settings.

Procedure

1. Click the Administration tab and click General in the left pane.
2. Modify the settings and click Apply.

General System Settings

vCloud Director includes general system settings that you can modify to meet your needs.
### Table 9-1. General System Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Start Time</td>
<td>LDAP Synchronization</td>
<td>Time of day to start LDAP synchronization.</td>
</tr>
<tr>
<td>Synchronization Interval</td>
<td>LDAP Synchronization</td>
<td>The number of hours between LDAP synchronizations.</td>
</tr>
<tr>
<td>Activity log history to keep</td>
<td>Activity Log</td>
<td>Number of days of log history to keep before deleting it. Type 0 to never delete logs.</td>
</tr>
<tr>
<td>Activity log history shown</td>
<td>Activity Log</td>
<td>Number of days of log history to display. Type 0 to show all activity.</td>
</tr>
<tr>
<td>Display debug information</td>
<td>Activity Log</td>
<td>Enable this setting to display debug information in the vCloud Director task log.</td>
</tr>
<tr>
<td>IP address release timeout</td>
<td>Networking</td>
<td>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.</td>
</tr>
<tr>
<td>Allow Overlapping External Networks</td>
<td>Networking</td>
<td>Select the check box to add external networks that run on the same network segment. Enable this setting only if you are using non-VLAN-based methods to isolate your external networks.</td>
</tr>
<tr>
<td>Default syslog server settings for networks</td>
<td>Networking</td>
<td>Type IP addresses for up to two Syslog servers for networks to use. This setting does not apply to Syslog servers used by cloud cells.</td>
</tr>
<tr>
<td>Provider Locale</td>
<td>Localization</td>
<td>Select a locale for provider activity, including log entries, email alerts, and so on.</td>
</tr>
<tr>
<td>Idle session timeout</td>
<td>Timeouts</td>
<td>Amount of time the vCloud Director application remains active without user interaction.</td>
</tr>
<tr>
<td>Maximum session timeout</td>
<td>Timeouts</td>
<td>Maximum amount of time the vCloud Director application remains active.</td>
</tr>
<tr>
<td>Host refresh frequency</td>
<td>Timeouts</td>
<td>How often vCloud Director checks whether its ESXi hosts are accessible or inaccessible.</td>
</tr>
<tr>
<td>Host hung timeout</td>
<td>Timeouts</td>
<td>Select the amount of time to wait before marking a host as hung.</td>
</tr>
<tr>
<td>Transfer session timeout</td>
<td>Timeouts</td>
<td>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.</td>
</tr>
<tr>
<td>Enable upload quarantine with a timeout of ___ seconds</td>
<td>Timeouts</td>
<td>Select the check box and enter a timeout number representing the amount of time to quarantine uploaded files.</td>
</tr>
<tr>
<td>Verify vCenter and vSphere SSO certificates</td>
<td>Certificates</td>
<td>Select the check box to allow vCloud Director to communicate only with trusted vCenter servers. Click Browse to locate the JCEKS keystore and type the keystore password.</td>
</tr>
</tbody>
</table>
Table 9-1. General System Settings (Continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify NSX Manager certificates</td>
<td>Certificates</td>
<td>Select the check box to allow vCloud Director to communicate only with trusted instances of NSX Manager. Click <strong>Browse</strong> to locate the JCEKS keystore and type the keystore password.</td>
</tr>
<tr>
<td>Maximum number of virtual data centers per organization</td>
<td>Organization VDC Limits</td>
<td>Type the maximum number of organization virtual data centers per organization, or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Number of resource intensive operations running per user</td>
<td>Operation Limits</td>
<td>Type the maximum number of simultaneous resource intensive operations per user, or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per user</td>
<td>Operation Limits</td>
<td>Type the maximum number of queued resource intensive operations per user, or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Number of resource intensive operations running per organization</td>
<td>Operation Limits</td>
<td>Type the maximum number of simultaneous resource intensive operations per organization, or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per organization</td>
<td>Operation Limits</td>
<td>Type the maximum number of queued resource intensive operations per organization, or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Provide default vApp names</td>
<td>Miscellaneous</td>
<td>Select the check box to configure vCloud Director to provide default names for new vApps.</td>
</tr>
<tr>
<td>Make Allocation pool Org VDCs elastic</td>
<td>Miscellaneous</td>
<td>Select the check box to enable elastic allocation pool, making all allocation pool organization virtual datacenters elastic. Before deselecting this option, ensure all virtual machines for each organization virtual datacenter have been migrated to a single cluster.</td>
</tr>
<tr>
<td>VM discovery enabled</td>
<td>Miscellaneous</td>
<td>By default, each organization VDC automatically discovers vCenter VMs that were created in any resource pool that backs the VDC. Clear to disable this for all VDC in the system.</td>
</tr>
</tbody>
</table>

**Editing System Email Settings**

You can edit system email settings, including SMTP and notification settings.

- **Configure SMTP Settings**
  vCloud Director requires an SMTP server to send user notifications and system alert emails to system users. Organizations can use the system SMTP settings, or use custom SMTP settings.

- **Configure System Notification Settings**
  vCloud Director sends system alert emails when it has important information to report. For example, vCloud Director sends an alert when a datastore is running out of space. You can configure vCloud Director to send email alerts to all system administrators or to a specified list of email addresses.

**Configure SMTP Settings**

vCloud Director requires an SMTP server to send user notifications and system alert emails to system users. Organizations can use the system SMTP settings, or use custom SMTP settings.
Procedure

1. Click the Administration tab and click Email in the left pane.
2. Type the DNS host name or IP address of the SMTP mail server.
3. Type the SMTP server port number.
4. (Optional) If the SMTP server requires a user name, select the Requires authentication check box and type the user name and password for the SMTP account.
5. Type an email address to appear as the sender for vCloud Director emails.
   vCloud Director uses the sender's email address to send runtime and storage lease expiration alerts.
6. Type text to use as the subject prefix for vCloud Director emails.
7. (Optional) Type a destination email address to test the SMTP settings and click Test SMTP settings.
8. Click Apply.

Configure System Notification Settings

vCloud Director sends system alert emails when it has important information to report. For example, vCloud Director sends an alert when a datastore is running out of space. You can configure vCloud Director to send email alerts to all system administrators or to a specified list of email addresses.

Organizations can use the system notification settings, or use custom notification settings.

Prerequisites

A valid connection to an SMTP server.

Procedure

1. Click the Administration tab and click Email in the left pane.
2. Select the recipients of system alert emails and click Apply.

Configuring Blocking Tasks and Notifications

Blocking tasks and notifications allow a system administrator to configure vCloud Director to send AMQP messages triggered by certain events.

Some of these messages are simply notifications that the event has occurred. These are known as notifications. Others publish information to a designated AMQP endpoint indicating that a requested action has been blocked pending action by a client program bound to that endpoint, and are known as blocking tasks.

A system administrator can configure a system-wide set of blocking tasks that are subject to programmatic action by an AMQP client.
Configure an AMQP Broker

You must configure an AMQP broker if you want vCloud Director to send AMQP messages triggered by certain events.

Procedure

1. Click the Administration tab and click Blocking Tasks in the left pane.
2. Click the Settings tab.
3. Type the DNS host name or IP address of the AMQP host.
   Type the AMQP port.
   The default port is 5672.
4. Type the exchange.
5. Type the vHost.
6. To use SSL, select the SSL check box and choose one of the certificate options.
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept all certificates</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Click Browse to locate the SSL certificate.</td>
</tr>
<tr>
<td>SSL Keystore</td>
<td>Click Browse to locate the SSL keystore. Type the keystore password.</td>
</tr>
</tbody>
</table>
   
   The CN record from the certificate owner field must match the AMQP broker host name. To use certificates that do not match the broker host name, select Accept all certificates.
7. Type a user name and password to connect to the AMQP host.
8. Click Test AMQP Connection to test the settings.
9. Click Apply.
10. (Optional) Select the Enable Notifications check box at the top of the page to publish audit events to the AMQP broker.

Configure Blocking Task Settings

You can specify status text, timeout settings, and default actions for blocking tasks. The settings apply to all organizations in the installation.

Procedure

1. Click the Administration tab and click Blocking Tasks in the left pane.
2. Click the Settings tab.
3. Select the default extension timeout.
4. Select the default timeout action.
Enable Blocking Tasks
You can configure certain tasks to be enabled for blocking tasks.

Procedure
1. Click the Administration tab and click Blocking Tasks in the left pane.
2. Click the Blocking Tasks tab.
3. Select the tasks to enable for blocking extensions.
4. Click Apply.

Configuring System LDAP Settings
You can configure vCloud Director to import user and group information from a supported LDAP service. System LDAP settings control how vCloud Director connects to an LDAP service, how often it synchronizes with that service, and how user and group names are mapped to LDAP attributes.

After you connect vCloud Director to an LDAP service, you can import system administrators from the groups and users in the LDAP directory. You can also use the system LDAP settings to import users and groups to an organization, or you can specify separate LDAP settings for each organization. An LDAP user cannot log in to vCloud Director until you import them to the system or an organization.

When an imported LDAP user logs in, vCloud Director validates the supplied credentials with the LDAP service and allows the login if the credentials are valid. vCloud Director cannot create or modify LDAP account information. You must use native LDAP tools to manage LDAP accounts.

Note  vCloud Director does not support hierarchical domains for LDAP authentication.

Supported LDAP Services
See the vCloud Director Release Notes for a list of LDAP services supported by this release of vCloud Director.

Configure an LDAP Connection
You can configure an LDAP connection to provide vCloud Director and its organizations with access to users and groups on the LDAP server.

Prerequisites
In order to use Kerberos as your authentication method, you must add a realm. See Add a Kerberos Realm.

Procedure
1. Click the Administration tab and click LDAP in the left pane.
2 Type the host name or IP address of the LDAP server.
   For Kerberos authentication, use the fully qualified domain name (FQDN).

3 Type a port number.
   For LDAP, the default port number is 389. For LDAP over SSL (LDAPS), the default port number is 636.

4 Type the base distinguished name (DN).
   The base DN is the location in the LDAP directory where vCloud Director connects. VMware recommends connecting at the root. Type the domain components only, for example, DC=example, DC=com.
   To connect to a node in the tree, type 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 vCloud Director.

5 Select the SSL check box to use LDAPS and choose one of the certificate options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept all certificates</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Click Browse to locate the SSL certificate.</td>
</tr>
<tr>
<td>SSL Keystore</td>
<td>Click Browse to locate the SSL keystore. Type and confirm the keystore password.</td>
</tr>
</tbody>
</table>

6 Select an authentication method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Simple authentication consists of sending the LDAP server the user's DN and password. If you are using LDAP, the LDAP password is sent over the network in clear text.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos issues authentication tickets to prove a user's identity. If you select Kerberos, you must select a realm.</td>
</tr>
</tbody>
</table>

7 Type a user name and password to connect to the LDAP server.
   If anonymous read support is enabled on your LDAP server, you can leave these text boxes blank.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>User Name Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Type the full LDAP DN.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Type the name in the form of <a href="mailto:user@REALM.com">user@REALM.com</a></td>
</tr>
</tbody>
</table>

8 Click **Apply**.

**What to do next**

You can now add LDAP users and groups to the system and to organizations that use the system LDAP settings.
Add a Kerberos Realm

vCloud Director requires a realm to use Kerberos authentication for an LDAP connection. You can add one or more realms for the system and its organizations to use. The system and each organization can only specify a single realm.

Prerequisites

You must select Kerberos as the authentication method before you can add a realm.

Procedure

1. Click the Administration tab and click LDAP in the left pane.
2. Click Edit All Realms.
3. (Optional) On the Realm tab, select Allow lower-case realms to allow realm names that include lower-case letters.
4. On the Realm tab, click Add.
5. Type a realm and its Key Distribution Center (KDC) and click OK.
   - If you did not choose to allow lower-case realms, the realm name must be all capital letters. For example, REALM.
6. On the DNS tab, click Add.
7. Type a DNS, select a realm, and click OK.
   - You can use the period (.) as a wildcard character in the DNS. For example, type .example.com.
8. Click Close and click Apply.

What to do next

You can now select a realm for the system LDAP settings or an organization's LDAP settings.

Test LDAP Settings

After you configure an LDAP connection, you can test its settings to make sure that user and group attributes are mapped correctly.

Prerequisites

You must configure an LDAP connection before you can test it.

Procedure

1. Click the Administration tab and click LDAP in the left pane.
2. Click Test LDAP Settings.
3. Type the name of a user in the LDAP directory and click Test.
4. Review the attribute mapping and click OK.
What to do next

You can customize LDAP user and group attributes based on the results of the test.

**Customize LDAP User and Group Attributes**

LDAP attributes provide vCloud Director with details about how user and group information is defined in the LDAP directory. vCloud Director maps the information to its own database. Modify the syntax for user and group attributes to match your LDAP directory.

**Prerequisites**

Verify that you have an LDAP connection

**Procedure**

1. Click the Administration tab and click LDAP in the left pane.
2. Modify the user and group attributes and click Apply.

**Synchronize vCloud Director with the LDAP Server**

vCloud Director automatically synchronizes its user and group information with the LDAP server on a regular basis. You can also manually synchronize with the LDAP server at any time.

For automatic synchronization, you can specify how often and when to synchronize. See Modify General System Settings.

**Prerequisites**

Verify that you have a valid LDAP connection.

**Procedure**

1. Click the Administration tab and click LDAP in the left pane.
2. Click Synchronize LDAP.

**Customize the vCloud Director Client UI**

You can customize the branding of the vCloud Director client UI and some of the links that appear on the vCloud Director Home login screen.

For a sample .css template with information about the styles that vCloud Director supports for custom themes, see http://kb.vmware.com/kb/1026050.

vCloud Director uses its default logo, or the logo that you upload, in the login screen, the header, and the footer. The login screen shows the logo in an area that ranges from a minimum of 48x48 pixels to a maximum of 60x150 pixels. You can upload logos that are smaller than 48x48 or larger than 60x150 and vCloud Director scales them to fit in the display area and maintain the aspect ratio of the uploaded image. The file size for an uploaded image cannot exceed 16384 bytes. The header and footer scale the logo to an appropriate size and maintain the aspect ratio of the original.
The file must be in the PNG, JPEG, or GIF format.

**Procedure**

1. Click the **Administration** tab and click **Branding** in the left pane.
2. Type a company name.
   - This name appears in the title bar for system administrators and in the footer for all users.
3. To select a custom logo, click **Browse**, select a file, and click **Open**.
4. To select a custom theme, click **Browse**, select a .css file, and click **Open**.
5. Type a URL that links to a Web site that provides information about your vCloud Director installation.
   - For example, [http://www.example.com](http://www.example.com). Users can follow the link by clicking the company name in the footer of the client UI.
6. Type a URL that links to a Web site that provides support for this vCloud Director installation.
   - The **Support** link on the **Home** tab of all vCloud Director organizations opens this URL.
7. Type a URL that links to a Web site that allows users to sign up for a vCloud Director account.
   - This link appears on the vCloud Director login page.
8. Type a URL that links to a Web site that allows users to recover their password.
   - This link appears on the vCloud Director login page.
9. Click **Apply**.

**Revert to System Default Logo**

If you uploaded a custom logo for vCloud Director, you can revert to the system default logo.

**Prerequisites**

Verify that you uploaded a custom logo.

**Procedure**

1. Click the **Administration** tab and click **Branding** in the left pane.
2. Select **Revert back to system default logo** and click **Apply**.

**Revert to System Default Theme**

If you applied a custom theme to vCloud Director, you can always revert to the system default theme.

**Prerequisites**

Verify that you previously applied a custom theme.

**Procedure**

1. Click the **Administration** tab and click **Branding** in the left pane.
Select Revert back to system default theme and click Apply.

Configuring Public Addresses

Public addresses are Web addresses exposed to clients of vCloud Director. Defaults for these addresses are specified during installation. A system administrator can update them if necessary.

In a vCloud Director that consists of a single cell, the public endpoints created by the installer are usually adequate to provide access for API and Web clients. Installations 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.

SSL Certificates for Customized Endpoints

The endpoints for the vCloud Director Tenant Portal and vCloud Director Web Console require SSL certificates, preferably signed. You must specify a path to these certificates when you install vCloud Director. If you customize any of these endpoints after installation, you might need to install new certificates that match endpoint details such as hostname and subject alternative name.

Customize Public Endpoints

The installer automatically configures endpoint Web addresses for the vCloud Director Web Console, vCloud API, Tenant Portal, and console proxy. A system administrator can customize these addresses if necessary to support load balancer or proxy requirements.

Prerequisites

Only the system administrator can customize public endpoints.

Procedure

1. Click the Administration tab and click Public Addresses in the left pane.
2. Select Customize Public Endpoints.
   - If you clear this checkbox, all endpoints revert to the defaults that were configured by the vCloud Director installer. Default values are not shown on this page.
3. Customize the vCloud API endpoints.
   - If you specify a custom value for HTTPS REST API base URL, click Browse to upload the certificates that establish the trust chain for that endpoint.
4. Customize the vCloud Director Web Console endpoints.
   - If you specify a custom value for vCloud Director secure public URL, click Browse to upload the certificates that establish the trust chain for that endpoint.
5 Customize the vCloud Director Tenant Portal endpoints.

Select Copy API URL Settings to configure the Tenant Portal to use the same endpoints and certificate chain you specified in Step 3.

6 Customize the vCloud Director public console proxy address.

This is the fully-qualified domain name of a cell host or load-balancer. The vCloud Director Web Console uses this address when opening a remote console window on a VM.

7 Click Apply to save your changes.

To discard your changes, click Revert.

Configure System Limits

Set limits for the maximum number of resource intensive operations, such as copy, move, Add to My Cloud, and Add to My Catalog, for the maximum number of console connections to a virtual machine, and for the maximum number of data centers per organization. These limits provide a defense against denial of service attacks.

Procedure

1 Click the Administration tab and click Policies in the left pane.

2 Choose the maximum system limits for resource intensive operations, console connections to a virtual machine, and data centers per organization.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of resource intensive operations per user</td>
<td>Type the maximum number of simultaneous resource intensive operations per user, or select Unlimited.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per user</td>
<td>Type the maximum number of queued resource intensive operations per user, or select Unlimited.</td>
</tr>
<tr>
<td>Number of resource intensive operations per organization</td>
<td>Type the maximum number of simultaneous resource intensive operations per organization, or select Unlimited.</td>
</tr>
<tr>
<td>Number of resource intensive operations to be queued per organization</td>
<td>Type the maximum number of queued resource intensive operations per organization, or select Unlimited.</td>
</tr>
<tr>
<td>Number of simultaneous connections per VM</td>
<td>Type the maximum number of simultaneous console connections per virtual machine, or select Unlimited.</td>
</tr>
<tr>
<td>Number of virtual data centers per organization</td>
<td>Type the maximum number of organization virtual data centers per organization, or select Unlimited.</td>
</tr>
</tbody>
</table>

3 (Optional) Click Revert to return all limits to the default system limit.

4 Click Apply to save the new system limits.

Configure the Account Lockout Policy

You can enable account lockout to prevent a user from logging in to the Web console after a certain number of failed attempts.
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. Click the **Administration** tab and click **Policies** in the left pane.
2. Select the **Account lockout enabled** check box, the **System Administrator account can lockout** check box, or both.
3. Select the number of invalid logins to accept before locking an account.
4. Select the lockout interval.
5. Click **Apply**.

**Configure vCloud Director to use the vSphere SSO SAML provider**

Configuring the System organization to use the vSphere SAML provider enables you to import system administrators from vSphere.

Using the vSphere SSO service as the SAML identity provider for the vCloud Director System organization can be a more secure alternative to LDAP or a local account. To use the vSphere SAML provider, you must have the credentials necessary to log in to vCloud Director and vSphere as an administrator, export each platform's SAML metadata to a local file on your client, and finally import that metadata into the SAML client on the other platform.

**Prerequisites**

This operation is restricted to system administrators.

You must also have the credentials needed to log in to vSphere as an SSO Administrator.

**Procedure**

1. Click the **Administration** tab and click **System Settings > Federation** in the left pane.
2. Download the vCloud Director SAML Service Provider metadata.
   a. In the **Service Provider** area of the **Federation** tab, verify the certificate expiration date.
      
      You can click **Regenerate** to regenerate the certificate and reset its expiration date.
      
      **Note** If you need to supply your own key and certificate chain, you can use the vCloud API.
   
   b. If the certificate expiration date meets your needs, click the **Metadata** link.
      
      The vCloud Director SAML Service Provider metadata (an XML file) downloads to the folder where your browser saves downloads.
3 Import the vCloud Director SAML metadata into vSphere.
   a Log in to the vSphere Web client as a vSphere SSO administrator.
   b Click Home > Administration to open the Administration menu, then click Single Sign-On > Configuration to display the SSO Configuration page.
   c Under SAML v2.0 Identity Providers, click the Import button to the right of Metadata from your SAML service provider.
   d On the Import Service Provider SAML Metadata page, click Import from File and browse the vCloud Director SAML metadata you downloaded in Step 2.

4 Download the VMware Identity provider metadata from vSphere.
   While you are still logged in to the vSphere Web client as a vSphere administrator, open the SSO Configuration page, then click the Download button to the right of Metadata for your SAML service provider. The vSphere SAML metadata (an XML file) downloads to the folder where your browser saves downloads.

5 Upload the vSphere identity provider metadata to vCloud Director
   In the Identity Provider area of the Federation tab, select Use SAML Identity Provider, then upload the vSphere SAML metadata you downloaded in Step 4. This completes the exchange of SAML metadata between vSphere and vCloud Director.

You can now import users from vSphere by selecting SAML in the Import Users dialog box. You can also use the Open in vSphere Web Client option to access vSphere resources on a vCenter Server in the same SSO domain.
Monitoring vCloud Director

System administrators can monitor completed and in-progress operations and view resource usage information at the provider virtual datacenter, organization virtual datacenter, and datastore level.

This chapter includes the following topics:

- Viewing Tasks and Events
- Monitor and Manage Blocking Tasks
- View Usage Information for a Provider Virtual Datacenter
- View Usage Information for an Organization Virtual Datacenter
- Using vCloud Director’s JMX Service
- Viewing the vCloud Director Logs
- vCloud Director and Cost Reporting

Viewing Tasks and Events

You can view system tasks and events and organization tasks and events to monitor and audit vCloud Directory activities.

vCloud Director tasks represent long-running operations and their status changes as the task progresses. For example, a task's status generally starts as Running. When the task finishes, its status changes to Successful or Error.

vCloud Director events represent one-time occurrences that typically indicate an important part of an operation or a significant state change for a vCloud Director object. For example, vCloud Director logs an event when a user initiates the creation an organization virtual datacenter and another event when the process completes. vCloud Director also logs an event every time a user logs in and notes whether the attempt was successful or not.

View Ongoing and Completed System Tasks

View the system log to monitor system-level tasks that are in progress, to find and troubleshoot failed tasks, and to view tasks by owner.

To view information about organization-level tasks, see View Ongoing and Completed Organization Tasks.
The log can also include debug information, depending on your vCloud Director settings. See General System Settings.

**Procedure**

1. Log in to the vCloud Director system as a system administrator.
2. Click the Manage & Monitor tab and click Logs in the left pane.
3. Click the Tasks tab.
   
   vCloud Director displays information about each system-level task.
4. Double-click a task for more information.

**View Ongoing and Completed Organization Tasks**

View the log for an organization to monitor organization-level tasks that are in progress, to find and troubleshoot failed tasks, and to view tasks by owner.

To view information about system-level tasks, see View Ongoing and Completed System Tasks.

The log can also include debug information, depending on your vCloud Director settings. See General System Settings.

**Procedure**

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3. Click the My Cloud tab and click Logs in the left pane.
4. Click the Tasks tab.
   
   vCloud Director displays information about each organization-level task.
5. Double-click a task for more information.
   
   Only system administrators can view the details about most tasks.

**View System Events**

View the system log to monitor system-level events. You can find and troubleshoot failed events and view events by user.

To view information about organization-level events, see View Organization Events.

**Procedure**

1. Log in to the vCloud Director system as a system administrator.
2. Click the Manage & Monitor tab and click Logs in the left pane.
3. Click the Events tab.
   
   vCloud Director displays information about each system-level event.
4 Double-click an event for more information.

**View Organization Events**

You can view the log for an organization to monitor organization-level events. You can find and troubleshoot failed events and view events by user.

To view information about system-level events, see View System Events.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
2 Right-click the organization name and select **Open**.
3 Click the **My Cloud** tab and click **Logs** in the left pane.
4 Click the **Events** tab.
   
   vCloud Director displays information about each organization-level event.
5 (Optional) Double-click an event for more information.
   
   Only system administrators can view the details about most events.

**View Ongoing and Completed Tenant Storage Migrations**

You can use the **Tenant Migration** tab on the **Logs** page to monitor and cancel tenant storage migrations.

A system administrator or other user in a role that includes the **Organization: Migrate Tenant Storage** right can migrate all of a tenant organization's vApps, independent disks, and catalog items to another datastore. Because tenant storage migration is a resource-intensive operation that can run for a long time, especially when the organization owns many assets, the system provides a way to view migration progress and cancel a migration. See **Migrate Tenant Storage**.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Logs** in the left pane.
2 Click the **Tenant Migration** tab.
   
   vCloud Director displays information about each queued or in-progress tenant storage migration.

**Monitor and Manage Blocking Tasks**

You can monitor and manage tasks that are in a pending state as a result of blocking.

Although, you can monitor and manage blocking tasks using the vCloud Director Web console, it is generally expected that an external piece of code will listen for AMQP notifications and programmatically respond using the vCloud API.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Blocking Tasks** in the left pane.
2 Right-click a task and select an action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resume</td>
<td>Resumes the task.</td>
</tr>
<tr>
<td>Abort</td>
<td>Aborts the task and deletes objects that were created as part of the task.</td>
</tr>
<tr>
<td>Fail</td>
<td>Fails the task but does not clean up objects that were created as part of the task. The status of the task and its objects is set to <em>Error</em>.</td>
</tr>
</tbody>
</table>

3 Type a reason and click **OK**.

**View Usage Information for a Provider Virtual Datacenter**

Provider virtual datacenters supply compute, memory, and storage resources to organization virtual datacenters. You can monitor provider virtual datacenter resources and add more resources if necessary.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Provider VDCs** in the left pane.

2 Click the **Monitor** tab.

vCloud Director displays information about CPU, memory, and storage for each provider virtual datacenter.

**View Usage Information for an Organization Virtual Datacenter**

Organization virtual datacenters supply compute, memory, and storage resources to organizations. You can monitor organization virtual datacenter resources and add more resources if necessary.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Organization VDCs** in the left pane.

2 Click the **Monitor** tab.

vCloud Director displays information about CPU, memory, and storage for each organization virtual datacenter.

**Using vCloud Director's JMX Service**

Each vCloud Director server host exposes a number of MBeans through JMX to allow for operational management of the server and to provide access to internal statistics.

**Access the JMX Service by Using JConsole**

You can use any JMX client to access the vCloud Director JMX service. JConsole is an example of a JMX client.

For more information about the MBeans exposed by vCloud Director, see [http://kb.vmware.com/kb/1026065](http://kb.vmware.com/kb/1026065).
Prerequisites

The host name of the vCloud Director host to which you connect must be resolvable by DNS using forward and reverse lookup of the fully-qualified domain name or the unqualified hostname.

Procedure

1. Start JConsole.
2. In the Connection menu, select New Connection.
3. Click Remote Process and type the JMX service URL.
   
   The URL consists of the host name or IP address of the vCloud Director server, followed by the port number. For example, example.com:8999. The default port is 8999.
4. Type a vCloud Director system administrator user name and password and click Connect.
5. Click the MBeans tab.

Viewing the vCloud Director Logs

vCloud Director provides logging information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues.

You can find the logs for a cell at /opt/vmware/vcloud-director/logs. Table 10-1 lists the available logs.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cell.log</td>
<td>Console output from the vCloud Director cell.</td>
</tr>
<tr>
<td>cell-management-tool</td>
<td>Cell Management Tool log messages from the cell.</td>
</tr>
<tr>
<td>cell-runtime</td>
<td>Runtime log messages from the cell.</td>
</tr>
<tr>
<td>cloud-proxy</td>
<td>Cloud proxy log messages from the cell.</td>
</tr>
<tr>
<td>console-proxy</td>
<td>Remote console proxy log messages from the cell.</td>
</tr>
<tr>
<td>server-group-communications</td>
<td>Server group communications from the cell.</td>
</tr>
<tr>
<td>statsfeeder</td>
<td>Virtual machine metric retrieval (from vCenter Server) and storage information and error messages.</td>
</tr>
<tr>
<td>vcloud-container-debug.log</td>
<td>Debug-level log messages from the cell.</td>
</tr>
<tr>
<td>vcloud-container-info.log</td>
<td>Informational log messages from the cell.</td>
</tr>
<tr>
<td>vmware-vcd-watchdog.log</td>
<td>Informational log messages from the cell watchdog. It records when the cell crashes, is restarted, and so on</td>
</tr>
<tr>
<td>diagnostics.log</td>
<td>Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.</td>
</tr>
<tr>
<td>YYYY_MM_DD.request.log</td>
<td>HTTP request logs in the Apache common log format.</td>
</tr>
</tbody>
</table>

You can use any text editor/viewer or third-party tool to view the logs.
vCloud Director and Cost Reporting

You can use VMware vCenter Chargeback Manager to configure a cost reporting system for VMware vCloud Director.

The cell management tool is a command-line utility that you can use to manage a vCloud Director cell or database. Superuser or system administrator credentials are required for most operations.

The cell management tool is installed in `/opt/vmware/vcloud-director/bin/cell-management-tool`. You can use it to execute a single command or run it as an interactive shell.

**Listing Available Commands**

To list the available cell management tool commands, use the following command line.

```bash
./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
```
### 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
```

- **Managing a Cell**
  
  Use the `cell` command of the cell management tool to suspend the task scheduler so that new tasks cannot be started, to check the status of active tasks, to control cell maintenance mode, and to shut down the cell gracefully.

- **Managing Cell Applications**
  
  Use the `cell-application` command of the cell management tool to control the set of applications that the cell runs on startup.

- **Exporting Database Tables**
  
  Use the `dbextract` command of the cell management tool to export data from the vCloud Director database.

- **Detecting and Repairing Corrupted Scheduler Data**
  
  vCloud 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.
- **Generating Self-Signed Certificates for the HTTP and Console Proxy Endpoints**
  Use the `generate-certs` command of the cell management tool to generate self-signed SSL certificates for the HTTP and Console Proxy endpoints.

- **Replacing Certificates for the HTTP and Console Proxy Endpoints**
  Use the `certificates` command of the cell management tool to replace SSL certificates for the HTTP and Console Proxy endpoints.

- **Importing SSL Certificates from External Services**
  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 vCloud Director database.

- **Managing the List of Allowed SSL Ciphers**
  Use the `ciphers` command of the cell management tool to configure the set of cipher suites that the cell offers to use during the SSL handshake process.

- **Managing the List of Allowed SSL Protocols**
  Use the `ssl-protocols` command of the cell management tool to configure the set of SSL protocols that the cell offers to use during the SSL handshake process.

- **Configuring Metrics Collection**
  Use the `configure-metrics` command of the cell management tool to configure the set of metrics to collect.

- **Configuring a Cassandra Metrics Database**
  Use the `cassandra` command of the cell management tool to connect the cell to an optional metrics database.

- **Recovering the System Administrator Password**
  If you know the vCloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the vCloud Director system administrator password.

- **Updating the Failure Status of a Task**
  Use the `fail-tasks` command of the 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**
  Use the `configure-audit-syslog` command of the cell management tool to configure the way the system logs audit messages.

- **Updating the Database Connection Properties**
  You can update the connection properties for the vCloud Director database by using the `reconfigure-database` subcommand of the cell management tool.
- **Configure a vCloud Director Installation**
  Use the `system-setup` command of the cell management tool to initialize the server group’s database with a system administrator account and related information.

- **Configure Email Templates**
  Use the `manage-email` command of the cell management tool to manage the templates that the system uses when creating email alerts.

- **Finding Orphaned VMs**
  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 vCloud Director database.

- **Join or Leave the VMware Customer Experience Improvement Program**
  Use the `configure-ceip` command of the cell management tool to join or leave the VMware Customer Experience Improvement Program (CEIP).

- **Migrate to a PostgreSQL Database**
  You can migrate an existing vCloud Director database from Oracle or Microsoft SQL Server to PostgreSQL by using the `dbmigrate` subcommand of the cell management tool.

### Managing a Cell

Use the `cell` command of the cell management tool to suspend the task scheduler so that new tasks cannot be started, to check the status of active tasks, to control cell maintenance mode, and to shut down the cell gracefully.

To manage a cell, use a command line with the following form:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell command
```

- **sysadmin-username**
  Username of a vCloud Director system administrator.

- **sysadmin-password**
  Password of the vCloud Director system administrator. You must quote the password if it contains special characters.

**Note** You can supply the vCloud Director system administrator password on the `cell-management-tool` command line, but it is more secure to omit the password. This causes the `cell-management-tool` to prompt for the password, which does not display on the screen as you type.

As an alternative to providing system administrator credentials, you can use the `--pid` option and provide the process ID of the cell process. To find the process ID of the cell, use a command like this one:

```
cat /var/run/vmware-vcd-cell.pid
```

- **command**
  cell subcommand.
<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--application-states (-a)</td>
<td>None</td>
<td>Display the state of each cell application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This subcommand is deprecated. See Managing Cell Applications for information about the cell-application subcommand.</td>
</tr>
<tr>
<td>--pid (-i)</td>
<td>Process ID of the cell process</td>
<td>You can use this option instead of -u or -u and -p.</td>
</tr>
<tr>
<td>--maintenance (-m)</td>
<td>true or false</td>
<td>Controls cell maintenance mode. The argument true puts the cell into maintenance mode. (You must quiesce the cell first.) The argument false releases the cell from maintenance mode.</td>
</tr>
<tr>
<td>--password (-p)</td>
<td>vCloud Director administrator password</td>
<td>Optional. The command will prompt for the password if you do not supply it on the command line.</td>
</tr>
<tr>
<td>--quiesce (-q)</td>
<td>true or false</td>
<td>Quiesces activity on the cell. The argument true suspends the scheduler. The argument false restarts the scheduler.</td>
</tr>
<tr>
<td>--shutdown (-s)</td>
<td>None</td>
<td>Shuts down vCloud Director services on the server.</td>
</tr>
<tr>
<td>--status (-t)</td>
<td>None</td>
<td>Displays information about the number of tasks running on the cell and the status of the cell.</td>
</tr>
<tr>
<td>--status-verbose (-tt)</td>
<td>None</td>
<td>Displays verbose information about the tasks running on the cell and the status of the cell.</td>
</tr>
<tr>
<td>--username (-u)</td>
<td>vCloud Director administrator user name.</td>
<td>Required if not specifying --pid.</td>
</tr>
</tbody>
</table>
Example: Getting Task Status

The following cell-management-tool command line supplies system administrator credentials and returns the count of running tasks. When the Job count value is 0 and the Is Active value is false, you can safely shut down the cell.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3
Is Active = true
In Maintenance Mode = false
```

Managing Cell Applications

Use the cell-application command of the cell management tool to control the set of applications that the cell runs on startup.

A vCloud Director runs a number of applications that provide services that vCloud Director clients require. The cell starts a subset of these applications by default. All members of that subset are typically required to support a vCloud Director installation.

To view or change the list of applications that run when the cell starts, use a command line with the following form:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

- **sysadmin-username**  Username of a vCloud Director system administrator.
- **sysadmin-password**  Password of the vCloud Director system administrator. You must quote the password if it contains special characters.

**Note**  You can supply the vCloud Director system administrator password on the cell-management-tool command line, but it is more secure to omit the password. This causes the cell-management-tool to prompt for the password, which does not display on the screen as you type.

As an alternative to providing system administrator credentials, you can use the --pid option and provide the process ID of the cell process. To find the process ID of the cell, use a command like this one:

```
cat /var/run/vmware-vcd-cell.pid
```

- **command**  cell-application subcommand.
Table 11-2. Cell Management Tool Options and Arguments, cell-application Subcommand

<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--application-states</td>
<td>None</td>
<td>List the cell applications and their current states.</td>
</tr>
<tr>
<td>--disable</td>
<td>Application ID</td>
<td>Prevent this cell application from running at cell startup.</td>
</tr>
<tr>
<td>--enable</td>
<td>Application ID</td>
<td>Enable this cell application to run at cell startup.</td>
</tr>
<tr>
<td>--pid (-i)</td>
<td>Process ID of the cell process</td>
<td>You can use this option instead of -u or -u and -p.</td>
</tr>
<tr>
<td>--list</td>
<td>None</td>
<td>List all cell applications and show whether they are enabled to run at cell startup.</td>
</tr>
<tr>
<td>--password (-p)</td>
<td>vCloud Director administrator password</td>
<td>Optional. The command will prompt for the password if you do not supply it on the command line.</td>
</tr>
<tr>
<td>--set</td>
<td>Semicolon-separated list of application IDs.</td>
<td>Specify the set of cell applications that run at cell startup. This command overwrites the existing set of cell applications that start at cell startup. Use --enable or --disable to change the startup state of a single application.</td>
</tr>
<tr>
<td>--username (-u)</td>
<td>vCloud Director administrator user name.</td>
<td>Required if not specifying --pid</td>
</tr>
</tbody>
</table>

Example: Listing Cell Applications and Their Startup States

The following cell-management-tool command line requires system administrator credentials and returns the list of cell applications and their startup states.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:
```

<table>
<thead>
<tr>
<th>name</th>
<th>id</th>
<th>enabled</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>com.vmware.vc...</td>
<td>true</td>
<td>Exposes NSX api endpoints directly from vCD.</td>
</tr>
<tr>
<td>Console Proxy</td>
<td>com.vmware.vc...</td>
<td>true</td>
<td>Proxies VM console data connection...</td>
</tr>
<tr>
<td>Cloud Proxy</td>
<td>com.vmware.vc...</td>
<td>true</td>
<td>Proxies TCP connections from a tenant site.</td>
</tr>
<tr>
<td>Compute Service Broker</td>
<td>com.vmware.vc...</td>
<td>true</td>
<td>Allows registering with a service control...</td>
</tr>
<tr>
<td>Maintenance Application</td>
<td>com.vmware.vc...</td>
<td>false</td>
<td>Indicates to users the cell is undergo ...</td>
</tr>
<tr>
<td>Core Cell Application</td>
<td>com.vmware.vc...</td>
<td>true</td>
<td>Main cell application, Flex UI and REST API.</td>
</tr>
</tbody>
</table>

Exporting Database Tables

Use the dbextract command of the cell management tool to export data from the vCloud Director database.

To export database tables, use a command line with the following form:

```
  cell-management-tool dbextract options
```
### Table 11-3. Cell Management Tool Options and Arguments, dbextract Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>-categories</td>
<td>A comma-separated list of table categories to export.</td>
<td>Optional. NETWORKING is the only supported category.</td>
</tr>
<tr>
<td>-dataFile</td>
<td>An absolute path to a file describing the data to export.</td>
<td>Optional. If not supplied, the command uses $VCLOUD_HOME/etc/data_to_export.properties. See Specifying Tables and Columns to Export.</td>
</tr>
<tr>
<td>-dumpFolder</td>
<td>An absolute path to the folder in which to create the dump. The folder must exist and be writable by vcloud.vcloud.</td>
<td>All data will be exported to a file in this folder.</td>
</tr>
<tr>
<td>-exportSettingsFile</td>
<td>An absolute path to a data export settings properties file.</td>
<td>Optional. If not supplied, the command uses $VCLOUD_HOME/etc/data_export_settings.ini. See Limiting and Ordering Exported Rows.</td>
</tr>
<tr>
<td>-properties</td>
<td>An absolute path to a database connection properties file.</td>
<td>Optional. If not supplied, the command uses the database connection properties in $VCLOUD_HOME/etc/global.properties. See Specifying a Properties File.</td>
</tr>
<tr>
<td>-tables</td>
<td>A comma-separated list of tables.</td>
<td>Optional. Export all tables to see individual table names.</td>
</tr>
</tbody>
</table>

### Specifying a Properties File

By default, the dbextract command extracts data from the vCloud Director database using the database connection information in the current cell's $VCLOUD_HOME/etc/global.properties file. To extract data from a different vCloud Director database, specify the database connection properties in a file and use the -properties option to provide the pathname to that file on the command line. The properties file is a UTF-8 file that has the following format.

```plaintext
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

- **username** The vCloud Director database user name.
- **password** The vCloud Director database password.
The database service name. For example, orcl.example.com.

The database port.

The IP address of the database server.

The database type. Must be Oracle or MS_SQL.

### Specifying Tables and Columns to Export

To restrict the set of data exported, use the `-exportSettingsFile` option and create a `data_to_export.properties` file that specifies individual tables and, optionally, columns to export. This file is a UTF-8 file that contains zero or more lines of the form `TABLE_NAME:COLUMN_NAME`.

**TABLE_NAME**

The name of a table in the database. To see a list of table names, export all tables.

**COLUMN_NAME**

The name of a column in the specified `TABLE_NAME`.

This example `data_to_export.properties` file exports columns from the ACL and ADDRESS_TRANSLATION tables.

```properties
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

The command expects to find this file in `$VCLOUND_HOME/etc/data_to_export.properties`, but you can specify another path.

### Limiting and Ordering Exported Rows

For any table, you can specify how many rows to export and how to order the exported rows. Use the `-exportSettingsFile` option and create a `data_export_settings.ini` file that specifies individual tables. This file is a UTF-8 file that contains zero or more entries of the following form:

```ini
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

**TABLE_NAME**

The name of a table in the database. To see a list of table names, export all tables.

**COLUMN_NAME**

The name of a column in the specified `TABLE_NAME`. 
This example data_export_settings.ini restricts data exported from the AUDIT_EVENT table to the first 10000 rows and orders the rows by the value in the event_time column.

```
[AUDIT_EVENT]
rowlimit=10000
orderby=event_time
```

The command expects to find this file in $VCLOUD_HOME/etc/data_export_settings.ini, but you can specify another path.

**Example: Exporting All Tables From the Current vCloud Director Database.**

This example exports all tables of the current vCloud Director database to the file /tmp/dbdump.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool dbextract --dumpFolder /tmp/dbdump
```

This utility outputs data from your vCloud Director system that may contain sensitive data.

Do you want to continue and output the data (y/n)?

```
y
```

Exporting data now. Please wait for the process to finish.

Exported 144 of 145 tables.

**Detecting and Repairing Corrupted Scheduler Data**

vCloud 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 11-4. Cell Management Tool Options and Arguments, fix-scheduler-data Subcommand**

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--dbuser</td>
<td>The user name of the vCloud Director database user.</td>
<td>Must be supplied on the command line.</td>
</tr>
<tr>
<td>--dbpassword</td>
<td>The password of the vCloud Director database user.</td>
<td>Prompted for if not supplied.</td>
</tr>
</tbody>
</table>
Generating Self-Signed Certificates for the HTTP and Console Proxy Endpoints

Use the `generate-certs` command of the cell management tool to generate self-signed SSL certificates for the HTTP and Console Proxy endpoints.

Each vCloud Director server group must support two SSL endpoints: one for the HTTP service and another for the console proxy service. The HTTP service endpoint supports the vCloud Director Web Console and the vCloud API. The remote console proxy endpoint supports VMRC connections to vApps and VMs.

The `generate-certs` command of the cell management tool automates the *Create a Self-Signed SSL Certificate* procedure shown in the *vCloud Director Installation and Upgrade Guide*.

To generate new self-signed SSL certificates and add them to a new or existing keystore, use a command line with the following form:

```
cell-management-tool generate-certs options
```

### Table 11.5. Cell Management Tool Options and Arguments, `generate-certs` Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--help (-h)</code></td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td><code>--expiration (-x)</code></td>
<td><code>days-until-expiration</code></td>
<td>Number of days until the certificates expire. Defaults to 365.</td>
</tr>
</tbody>
</table>
| `--issuer (-i)` | `name=value [,
name=value, ...]` | X.509 distinguished name of the certificate issuer. Defaults to
`CN=FQDN`, where `FQDN` is the fully-qualified domain name of the cell or
its IP address if no fully-qualified domain name is available. If you
specify multiple attribute and value pairs, separate them with commas
and enclose the entire argument in quotation marks. |
| `--httpcert (-j)` | None | Generate a certificate for the http endpoint. |
| `--key-size (-s)` | `key-size` | Size of key pair expressed as an integer number of bits. Defaults to
2048. Note that key sizes smaller
than 1024 are no longer supported per NIST Special Publication 800-131A. |
| `--keystore-pwd (-w)` | `keystore-password` | Password for the keystore on this host. |
Table 11-5. Cell Management Tool Options and Arguments, generate-certs Subcommand (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--out (-o)</td>
<td>keystore-pathname</td>
<td>Full pathname to the keystore on this host.</td>
</tr>
<tr>
<td>--consoleproxycert (-p)</td>
<td>None</td>
<td>Generate a certificate for the console proxy endpoint.</td>
</tr>
</tbody>
</table>

**Note** To maintain compatibility with previous releases of this subcommand, omitting both \(-j\) and \(-p\) has the same result as supplying both \(-j\) and \(-p\).

**Example: Creating Self-Signed Certificates**

Both of these examples assume a keystore at /tmp/cell.ks that has the password kspw. This keystore is created if it does not already exist.

This example creates the new certificates using the defaults. The issuer name is set to CN=Unknown. The certificate uses the default 2048-bit key length and expires one year after creation.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

This example creates a new certificate for the http endpoint only. It also specifies custom values for key size and issuer name. The issuer name is set to CN=Test, L=London, C=GB. The new certificate for the http connection has a 4096 bit key and expires 90 days after creation. The existing certificate for the console proxy endpoint is unaffected.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

**Important** The keystore file and the directory in which it is stored must be readable by the user vcloud.vcloud. The vCloud Director installer creates this user and group.

**Replacing Certificates for the HTTP and Console Proxy Endpoints**

Use the certificates command of the cell management tool to replace SSL certificates for the HTTP and Console Proxy endpoints.
The certificates command of the cell management tool automates the process of replacing existing certificates with new ones stored in a JCEKS keystore. Use the certificates command to replace self-signed certificates with signed ones or replace expiring certificates with new ones. To create a JCEKS keystore containing signed certificates, see *Create a Self-Signed SSL Certificate* in the *vCloud Director Installation and Upgrade Guide*.

To replace SSL certificates for one or both endpoints use a command with the following form:

```
cell-management-tool certificates options
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--config (-c)</td>
<td>full pathname to the cell's</td>
<td>Defaults to $VCLOUD_HOME/etc/global.properties.</td>
</tr>
<tr>
<td></td>
<td>global.properties file</td>
<td></td>
</tr>
<tr>
<td>--httpks (-j)</td>
<td>None</td>
<td>Replace the keystore file named certificates used by the http endpoint.</td>
</tr>
<tr>
<td>--consoleproxyks (-p)</td>
<td>None</td>
<td>Replace the keystore file named proxycertificates used by the console proxy endpoint.</td>
</tr>
<tr>
<td>--responses (-r)</td>
<td>full pathname to the cell's</td>
<td>Defaults to $VCLOUD_HOME/etc/responses.properties.</td>
</tr>
<tr>
<td></td>
<td>responses.properties file</td>
<td></td>
</tr>
<tr>
<td>--keystore (-k)</td>
<td>keystore-pathname</td>
<td>Full pathname to a JCEKS keystore containing the signed certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deprecated --s short form replaced by --k.</td>
</tr>
<tr>
<td>--keystore-password (-w)</td>
<td>keystore-password</td>
<td>Password for the JCEKS keystore referenced by the --keystore option. Replaces deprecated --kspassword and --keystorepwd options.</td>
</tr>
</tbody>
</table>
Example: Replacing Certificates

You can omit the --config and --responses options unless those files were moved from their default locations. In this example, a keystore at /tmp/my-new-certs.ks has the password kspw. This example replaces the cell's existing http endpoint certificate with the one found in /tmp/my-new-certs.ks

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

**Note** You must restart the cell after you replace the certificates.

Importing SSL Certificates from External Services

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 vCloud Director database.

Before it can make a secure connection to an external service, vCloud 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 11-7. Cell Management Tool Options and Arguments, import-trusted-certificates Subcommand**

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--destination</td>
<td>path name</td>
<td>Full path name to the destination truststore. Defaults to /opt/vmware/vcloud-director/jre/lib/security/cacerts if not provided on the command line.</td>
</tr>
<tr>
<td>--destination-password</td>
<td>string</td>
<td>Keystore password for the keystore in --destination. If --destination is omitted or set to the default JRE keystore (/opt/vmware/vcloud-director/jre/lib/security/cacerts), the password defaults to changeit if not provided on the command line.</td>
</tr>
<tr>
<td>--destination-type</td>
<td>keystore type</td>
<td>One of JKS, JCEKS (default)</td>
</tr>
</tbody>
</table>

VMware, Inc.
Table 11-7. Cell Management Tool Options and Arguments, import-trusted-certificates Subcommand (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force</td>
<td>None</td>
<td>Overwrite any existing certificate in --destination.</td>
</tr>
<tr>
<td>--private-key-path</td>
<td>Absolute path of private key that has had its public key added to the authorized_keys of other cells in the server group.</td>
<td>When you use this option and the --source path name is accessible by all cells, the specified certificate is imported into all cells in the server group.</td>
</tr>
<tr>
<td>--source</td>
<td>path name</td>
<td>Full path name to source PEM file.</td>
</tr>
</tbody>
</table>

Example: Importing Trusted Certificates

This example imports the certificates found at /tmp/demo.pem to the system's default keystore. Because the --destination option specifies the default keystore for the system JRE and the keystore password is not supplied on the command line, the system uses the default password defined by the system JRE.

[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem --destination /opt/vmware/vcloud-director/jre/lib/security/cacerts
Successfully stored certificates in truststore.

Managing the List of Allowed SSL Ciphers

Use the ciphers command of the cell management tool to configure the set of cipher suites that the cell offers to use during the SSL handshake process.

When a client makes an SSL connection to a vCloud Director cell, the cell offers to use only those ciphers that are configured on its default list of allowed ciphers. Several ciphers are not on this list, either because they are not strong enough to secure the connection, or because they are known to contribute to SSL connection failures. When you install or upgrade vCloud Director, the installation or upgrade script examines the cell's certificates. If any of the certificates are encrypted using a cipher that is not on the list of allowed ciphers, the script modifies the cell's configuration to allow use of that cipher and displays a warning. You can continue using the existing certificates despite their dependence on these ciphers, or you can take the following steps to replace the certificates and reconfigure the list of allowed ciphers:

1. Create new certificates that do not use any of the disallowed ciphers. You can use cell-management-tool ciphers -a as shown in Example: List All Allowed Ciphers to list all the ciphers that are allowed in the default configuration.

2. Use the cell-management-tool certificates command to replace the cell's existing certificates with the new ones.
3 Use the `cell-management-tool ciphers` command to reconfigure the list of allowed ciphers to exclude any ciphers not used by the new certificates. Excluding these ciphers can make it faster to establish an SSL connection to the cell, since the number of ciphers offered during the handshake is reduced to the practical minimum.

**Important** Because the VMRC console requires the use of the AES256-SHA and AES128-SHA ciphers, you cannot disallow them if your vCloud Director clients use the VMRC console.

To manage the list of allowed SSL ciphers, use a command line with the following form:

```
cell-management-tool ciphers options
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--all-allowed (-a)</td>
<td>None</td>
<td>List all allowed ciphers.</td>
</tr>
<tr>
<td>--compatible-reset (-c)</td>
<td>None</td>
<td>Reset to default list of allowed ciphers, and also allow ciphers used by this cell's certificates.</td>
</tr>
<tr>
<td>--disallow (-d)</td>
<td>Comma-separated list of cipher names, as published at <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a></td>
<td>Disallow the ciphers in specified comma-separated list.</td>
</tr>
<tr>
<td>--list (-l)</td>
<td>None</td>
<td>List currently configured ciphers.</td>
</tr>
<tr>
<td>--reset (-r)</td>
<td>None</td>
<td>Reset to default list of allowed ciphers. If this cell's certificates use disallowed ciphers, you will not be able to make an SSL connection to the cell until you install new certificates that use an allowed cipher.</td>
</tr>
</tbody>
</table>

**Example: List All Allowed Ciphers**

Use the `--all-allowed (-a)` option to list all the ciphers that the cell is currently allowed to offer during an SSL handshake.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
```
Example: Disallow Two Ciphers

Use the `--disallow (-d)` option to remove one or more ciphers from the list of allowed ciphers. This option requires at least one cipher name. You can supply multiple cipher names in a comma-separated list. You can obtain names for this list from the output of `ciphers --a`. This example removes two ciphers listed in the previous example.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Managing the List of Allowed SSL Protocols

Use the `ssl-protocols` command of the cell management tool to configure the set of SSL protocols that the cell offers to use during the SSL handshake process.

When a client makes an SSL connection to a vCloud Director cell, the cell offers to use only those protocols that are configured on its list of allowed SSL protocols. Several protocols, including TLSv1, SSLv3 and SSLv2Hello, are not on the default list because they are known to have serious security vulnerabilities.

To manage the list of allowed SSL protocols, use a command line with the following form:

```
cell-management-tool ssl-protocols options
```
Table 11-9. Cell Management Tool Options and Arguments, ssl-protocols Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--all-allowed (-a)</td>
<td>None</td>
<td>List all SSL protocols that vCloud Director is able to support.</td>
</tr>
<tr>
<td>--disallow (-d)</td>
<td>Comma-separated list of SSL protocol names.</td>
<td>Reconfigure the list of disallowed SSL protocols to the ones specified in the list.</td>
</tr>
<tr>
<td>--list (-l)</td>
<td>None</td>
<td>List the set of allowed SSL protocols that vCloud Director is currently configured to support.</td>
</tr>
<tr>
<td>--reset (-r)</td>
<td>None</td>
<td>Reset the list of configured SSL protocols to the factory default</td>
</tr>
</tbody>
</table>

**Important**  You must re-start the cell after running `ssl-protocols --disallow` or `ssl-protocols reset`.

**Example: List Allowed and Configured SSL Protocols**

Use the `--all-allowed (-a)` option to list all the SSL protocols that the cell can be allowed to offer during an SSL handshake.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

This list is typically a superset of the SSL protocols that the cell is configured to support. To list those SSL protocols, use the `--list (-l)` option.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

**Example: Reconfigure the List of Disallowed SSL Protocols**

Use the `--disallow (-d)` option to reconfigure the list of disallowed SSL protocols. This option requires a comma-separated list of the subset of allowed protocols produced by `ssl-protocols -a`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols --disallow
```
This example updates the list of allowed SSL protocols to include TLSv1. VMware® vCenter™ releases earlier than 5.5 Update 3e require TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

You must re-start the cell after running this command.

### Configuring Metrics Collection

Use the `configure-metrics` command of the cell management tool to configure the set of metrics to collect.

vCloud Director can collect metrics that provide current and historic information about virtual machine performance and resource consumption. Use this subcommand to configure the metrics that vCloud Director collects. Use the `cell-management-tool cassandra` subcommand to configure an Apache Cassandra database for use as a vCloud Director metrics repository. See Configuring a Cassandra Metrics Database.

To configure the metrics that vCloud Director collects, use a command line with the following form:

```
cell-management-tool configure-metrics --metrics-config pathname
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--repository-host (Deprecated)</td>
<td>Host name or IP address of KairosDB host</td>
<td>Deprecated. Use the --cluster-nodes option of the <code>cell-management-tool cassandra</code> subcommand to configure an Apache Cassandra database for use as a vCloud Director metrics repository.</td>
</tr>
<tr>
<td>--repository-port (Deprecated)</td>
<td>KairosDB port to use.</td>
<td>Deprecated. Use the --port option of the <code>cell-management-tool cassandra</code> subcommand to configure an Apache Cassandra database for use as a vCloud Director metrics repository.</td>
</tr>
<tr>
<td>--metrics-config</td>
<td>path name</td>
<td>Path to metrics configuration file</td>
</tr>
</tbody>
</table>

### 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 vCloud 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:

```plaintext
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 11-11. Metric Names**

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu.usage.average</td>
<td>Host view of this virtual machine’s average actively used CPU as a percentage of total available. Includes all cores in all sockets.</td>
</tr>
<tr>
<td>cpu.usagemhz.average</td>
<td>Host view of this virtual machine’s average actively used CPU as a raw measurement. Includes all cores in all sockets.</td>
</tr>
<tr>
<td>cpu.usage.maximum</td>
<td>Host view of this virtual machine’s maximum actively used CPU as a percentage of total available. Includes all cores in all sockets.</td>
</tr>
<tr>
<td>mem.usage.average</td>
<td>Memory used by this virtual machine as a percentage of total configured memory.</td>
</tr>
<tr>
<td>disk.provisioned.latest</td>
<td>Storage space allocated to this virtual hard disk in the containing organization virtual data center.</td>
</tr>
<tr>
<td>disk.used.latest</td>
<td>Storage used by all virtual hard disks.</td>
</tr>
<tr>
<td>disk.read.average</td>
<td>Average read rate for all virtual hard disks.</td>
</tr>
<tr>
<td>disk.write.average</td>
<td>Average write rate for all virtual hard disks.</td>
</tr>
</tbody>
</table>

**Note** When a virtual machine has multiple disks, metrics are reported 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 11-12. Metrics Collection Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>currentInterval</td>
<td>Integer number of seconds.</td>
<td>The interval in seconds to use when querying for the latest available metric values (for current metrics queries) Defaults to 20 if not specified. Values greater than 20 are supported only for Level 1 metrics as defined by the vSphere Performance Manager.</td>
</tr>
<tr>
<td>historicInterval</td>
<td>Integer number of seconds.</td>
<td>The interval in seconds to use when querying for historic metric values. Defaults to 20 if not specified. Values greater than 20 are supported only for Level 1 metrics as defined by the vSphere Performance Manager.</td>
</tr>
<tr>
<td>entity</td>
<td>One of: HOST, VM</td>
<td>The type of VC object that the metric is available for Defaults to VM if not specified. Not all metrics are available for all entities.</td>
</tr>
<tr>
<td>instance</td>
<td>A vSphere Performance Manager PerfMetricId instance identifier.</td>
<td>Indicates whether to retrieve data for individual instances of a metric (individual CPU cores for example), an aggregate of all instances, or both. A value of &quot;<em>&quot; collects all metrics, instance and aggregate. An empty string, &quot;&quot; collects only the aggregate data. A specific string like &quot;DISKFILE&quot; collects data only for that instance. Defaults to &quot;</em>&quot; if not specified.</td>
</tr>
<tr>
<td>minReportingInterval</td>
<td>Integer number of seconds.</td>
<td>Specifies a default aggregation interval in seconds to use when reporting time series data. Provides further control over reporting granularity when the collection interval's granularity is not sufficient. Defaults to 0 (no dedicated reporting interval)</td>
</tr>
<tr>
<td>aggregator</td>
<td>One of: AVERAGE, MINIMUM, MAXIMUM, SUMMATION</td>
<td>The type of aggregation to perform during the minReportingInterval. Defaults to AVERAGE if not specified.</td>
</tr>
</tbody>
</table>

Configuring a Cassandra Metrics Database

Use the cassandra command of the cell management tool to connect the cell to an optional metrics database.

vCloud 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 vCloud Director metrics repository. Use the cell-management-tool configure-metrics subcommand to tool to configure the set of metrics to collect. See Configuring Metrics Collection.

Data for historic metrics is stored in an Apache Cassandra database. See the vCloud Director Installation and Upgrade Guide for more information about configuring optional database software to store and retrieve performance metrics.

To create a connection between vCloud Director and an Apache Cassandra database, use a command line with the following form:

cell-management-tool cassandra options
### Table 11-13. Cell Management Tool Options and Arguments, cassandra Subcommand

<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available options for this command.</td>
</tr>
<tr>
<td>--cluster-nodes</td>
<td>address</td>
<td>Comma-separated list of Cassandra cluster nodes to use for vCloud Director metrics.</td>
</tr>
<tr>
<td>--clean</td>
<td>None</td>
<td>Remove Cassandra configuration settings from the vCloud Director database.</td>
</tr>
<tr>
<td>--configure</td>
<td>None</td>
<td>Configure vCloud Director for use with an existing Cassandra cluster.</td>
</tr>
<tr>
<td>--dump</td>
<td>None</td>
<td>Dump the current connection configuration.</td>
</tr>
<tr>
<td>--keyspace</td>
<td>string</td>
<td>Set vCloud Director keyspace name in Cassandra to string. Defaults to vcloud_metrics.</td>
</tr>
<tr>
<td>--offline</td>
<td>None</td>
<td>Configure Cassandra for use by vCloud Director, but do not test the configuration by connection to vCloud Director.</td>
</tr>
<tr>
<td>--password</td>
<td>string</td>
<td>Password of Cassandra database user</td>
</tr>
<tr>
<td>--port</td>
<td>integer</td>
<td>Port to connect to at each cluster node. Defaults to 9042.</td>
</tr>
<tr>
<td>--ttl</td>
<td>integer</td>
<td>Retain metrics data for integer days. Set integer to 0 to retain metrics data forever.</td>
</tr>
<tr>
<td>--update-schema</td>
<td>None</td>
<td>Initializes the Cassandra schema to hold vCloud Director metrics data.</td>
</tr>
<tr>
<td>--username</td>
<td>string</td>
<td>User name of the Cassandra database user</td>
</tr>
</tbody>
</table>

### 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 are 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 re-start the cell after this command completes.
Recovering the System Administrator Password

If you know the vCloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the vCloud Director system administrator password.

With the `recover-password` command of the cell management tool, a user who knows the vCloud Director database username and password can recover the vCloud 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 11-14. Cell Management Tool Options and Arguments, `recover-password` Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--help (-h)</code></td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td><code>--dbuser</code></td>
<td>The user name of the vCloud Director database user.</td>
<td>Must be supplied on the command line.</td>
</tr>
<tr>
<td><code>--dbpassword</code></td>
<td>The password of the vCloud Director database user.</td>
<td>Prompted for if not supplied.</td>
</tr>
</tbody>
</table>

Update the Failure Status of a Task

Use the `fail-tasks` command of the 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 11-15. Cell Management Tool Options and Arguments, fail-tasks Subcommand

<table>
<thead>
<tr>
<th>Command</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--message (-m)</td>
<td>Message text.</td>
<td>Message text to place in task completion status.</td>
</tr>
</tbody>
</table>

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

Use the configure-audit-syslog command of the cell management tool to configure the way the system logs audit messages.

Services in each vCloud Director cell log audit messages to the vCloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure vCloud Director services to send audit messages to the Linux syslog utility in addition to the vCloud Director database.

The system configuration script allows you to specify how audit messages are handled. See "Configure Network and Database Connections" in the vCloud Director Installation 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-tool configure-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 11-16. Cell Management Tool Options and Arguments, configure-audit-syslog Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--disable (-d)</td>
<td>None</td>
<td>Disable logging of audit events to syslog. Log audit events only to the vCloud Director database. This option unsets the values of the audit.syslog.host and audit.syslog.port properties in global.properties and responses.properties.</td>
</tr>
<tr>
<td>--syslog-host (-loghost)</td>
<td>IP address or fully-qualified domain name of the syslog server host</td>
<td>This option sets the value of the audit.syslog.host property to the specified address or fully-qualified domain name.</td>
</tr>
<tr>
<td>--syslog-port (-logport)</td>
<td>integer in the range 0-65535</td>
<td>This option sets the value of the audit.syslog.port property to the specified integer.</td>
</tr>
</tbody>
</table>

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 file is in place (in /opt/vmware/vcloud-director/etc/responses.properties) and writeable. See "Protecting and Reusing the Response File" in the vCloud Director Installation 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.

**Updating the Database Connection Properties**

You can update the connection properties for the vCloud Director database by using the reconfigure-database subcommand of the cell management tool.
During the vCloud Director installation process, you run a configuration script or perform an unattended configuration where you set the database type and database connections properties. For information about configuring network and database connections, see *vCloud Director Installation and Upgrade Guide*.

After finishing the vCloud Director installation, you can update the database connections by using the `reconfigure-database` subcommand. You can move the existing vCloud Director database to a new host, change the database user name or password, or enable an SSL connection to a PostgreSQL database.

After finishing the vCloud Director installation, you can also change the database type by migrating the database from Oracle or Microsoft SQL Server to PostgreSQL. See *Migrate to a PostgreSQL Database*. If you migrate the database without reconfiguring the cells in the group, you can use the `reconfigure-database` subcommand to connect the cells to the target PostgreSQL database.

[cell-management-tool reconfigure-database options]

**Important** The changes you make by running the `reconfigure-database` command are written to the global configuration file `global.properties` and the response file `responses.properties` of the cell. Before you run the command, verify that the response file is present at `/opt/vmware/vcloud-director/etc/responses.properties` and writable. For information about protecting and reusing the response file, see *vCloud Director Installation and Upgrade Guide*.

To apply the changes, you must restart the cell.

**Table 11-17. Cell Management Tool Options and Arguments, reconfigure-database Subcommand**

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--database-host (-dbhost)</td>
<td>IP address or fully qualified domain name of the vCloud Director database host</td>
<td>Updates the value of the <code>database.jdbcUrl</code> property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important</strong> The command validates only the value format.</td>
</tr>
<tr>
<td>--database-instance (-dbinstance)</td>
<td>SQL Server database instance.</td>
<td>Optional if database type is sqlserver.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important</strong> If you include this option, you must provide the same value that you specified when you originally ran the configuration script.</td>
</tr>
</tbody>
</table>
Table 11-17. Cell Management Tool Options and Arguments, reconfigure-database Subcommand (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--database-name</td>
<td>The database service name. For information about installing and configuring a vCloud Director database, see vCloud Director Installation and Upgrade Guide.</td>
<td>Updates the value of the database.jdbcUrl property.</td>
</tr>
<tr>
<td>(-dbname)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--database-pwd</td>
<td>Password for the database user.</td>
<td>Updates the value of the database.password property. The password you supply is encrypted before it is stored as a property value.</td>
</tr>
<tr>
<td>(-dbpassword)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--database-port</td>
<td>Port number used by the database service on the database host.</td>
<td>Updates the value for the database.jdbcUrl property.</td>
</tr>
<tr>
<td>(-dbport)</td>
<td></td>
<td>Important The command validates only the value format.</td>
</tr>
<tr>
<td>--database-type</td>
<td>The database type. One of: oracle, sqlserver, postgres</td>
<td>Updates the value of the database.jdbcUrl property.</td>
</tr>
<tr>
<td>(-dbtype)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--database-user</td>
<td>User name of the database user.</td>
<td>Updates the value of the database.user property.</td>
</tr>
<tr>
<td>(-dbuser)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--database-ssl</td>
<td>true or false</td>
<td>Configures the target PostgreSQL database to require an SSL connection from vCloud Director.</td>
</tr>
<tr>
<td>--private-key-path</td>
<td>Pathname to the private key of the cell.</td>
<td>All cells in the server group gracefully shut down, update their database properties, and restart.</td>
</tr>
</tbody>
</table>

When you use options --database-host and --database-port, the command validates the format of the arguments but does not test the combination of host and port for network accessibility or the presence of a running database of the specified type.
If you use the --private-key-path option, all cells must be configured to permit SSH connections from
the superuser without a password. To perform a verification, for example, you can run the following Linux
command:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

This example sets your identity to vcloud, then makes an SSH connection to the cell at cell-ip as root but
does not supply the root password. If the private key in private-key-path on the local cell is readable by
user vcloud.vcloud and the corresponding public key is present in the authorized-keys file for the
root user at cell-ip, the command succeeds.

**Note** The vcloud user, vcloud group, and vcloud.vcloud account are created by the vCloud Director
installer for use as an identity with which vCloud Director processes run. The vcloud user has no
password.

**Example: Change the vCloud Director Database User Name and Password**

To change the vCloud Director database user name and password, leaving all other connection properties
as they were originally configured, you can run the following command:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database
      -dbuser vcd-dba -dbpassword P@55w0rd
```

**Example: Reconfigure a Cell After Migrating the vCloud Director
Database to PostgreSQL**

If you migrated the vCloud Director database from Oracle or Microsoft SQL Server to PostgreSQL without
reconfiguring the cells in the server group, to connect each cell to the new PostgreSQL database, you
can run the following command:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database
      -dbhost psql.example.com -dbport 5432 -dbuser vcd-dba -dbname vcloud -dbpassword P@55w0rd
      -dbtype postgres
```

**Configure a vCloud Director Installation**

Use the system-setup command of the cell management tool to initialize the server group's database
with a system administrator account and related information.
The `system-setup` command is a command-line alternative to the vCloud Director Setup wizard described in the *vCloud Director Installation and Upgrade Guide*. After you configure all servers in the vCloud Director server group and connect them to the database, you can create the initial system administrator account and initialize the vCloud Director database with related information with a command line of the following form:

```bash
cell-management-tool system-setup options
```

You cannot run this command on a system that has already been set up. All options except `--unattended` and `--password` must be specified.

### Table 11-18. Cell Management Tool Options and Arguments, `system-setup` Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--help (-h)</code></td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td><code>--email</code></td>
<td>The e-mail address for the system administrator you are creating.</td>
<td>The system administrator's email address is stored in the vCloud Director database.</td>
</tr>
<tr>
<td><code>--full-name</code></td>
<td>The full name of the system administrator you are creating.</td>
<td>The system administrator's full name is stored in the vCloud Director database.</td>
</tr>
<tr>
<td><code>--installation-id</code></td>
<td>An integer in the range 1-63</td>
<td>The installation ID for this installation of vCloud Director. If a datacenter includes multiple installations of vCloud Director, each installation must specify a unique installation ID. The system uses the installation ID when generating MAC addresses for virtual NICs.</td>
</tr>
<tr>
<td><code>--password</code></td>
<td>The password for the system administrator you are creating. Required when you use the <code>--unattended</code> option. If you do not use the <code>--unattended</code> option, the command prompts you for this password if you do not supply it on the command line.</td>
<td>The system administrator supplies this password when authenticating to vCloud Director.</td>
</tr>
<tr>
<td><code>--serial-number</code></td>
<td>The serial number (license key) for this installation.</td>
<td>Optional. Must be a valid vCloud Director serial number if supplied.</td>
</tr>
<tr>
<td><code>--system-name</code></td>
<td>The name to use a name for the vCloud Director vCenter Server folder.</td>
<td>This vCloud Director installation is represented by a folder with this name in each vCenter Server with which it registers.</td>
</tr>
</tbody>
</table>
Table 11-18. Cell Management Tool Options and Arguments, system-setup Subcommand (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--unattended</td>
<td>None</td>
<td>Optional. The command does not prompt for further input when invoked with this option.</td>
</tr>
<tr>
<td>--user</td>
<td>The user name of the system administrator you are creating.</td>
<td>The system administrator supplies this user name when authenticating to vCloud Director.</td>
</tr>
</tbody>
</table>

Example: Specify vCloud Director System Settings

A command like this one specifies all system settings for a new vCloud Director installation. Because --unattended and --password are not specified, the command prompts you to supply and confirm the password to create for the system administrator.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \
--user admin --full-name "VCD System Administrator" --email vcd-admin@example.com --system-name VCD -- \
installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]: y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

Configure Email Templates

Use the manage-email command of the cell management tool to manage the templates that the system uses when creating email alerts.

The system is configured by default to send 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 vCloud 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 11-19. Cell Management Tool Options and Arguments, manage-email Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--delete</td>
<td>template name</td>
<td>The name of the template to delete.</td>
</tr>
<tr>
<td>--lookup</td>
<td>template name</td>
<td>This argument is optional. If you do not supply it, the command returns a list of all template names.</td>
</tr>
<tr>
<td>--locale</td>
<td>the template locale</td>
<td>By default, this command operates on templates in the en-US locale. Use this option to specify a different locale.</td>
</tr>
<tr>
<td>--set-template</td>
<td>path name to a file containing an updated email template</td>
<td>This file must be accessible on the local host and readable by the user vcloud.vcloud. For example, /tmp/my-email-template.txt</td>
</tr>
</tbody>
</table>

Example: Update an email Template

The following command replaces the current contents of the DISK_STORAGE_ALERT email template with content you created in a file named /tmp/DISK_STORAGE_ALERT-new.txt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#/cell-management-tool manage-email --set-template DISK_STORAGE_ALERT /tmp/DISK_STORAGE_ALERT-new.txt
```

New property being stored: Property "email.template.DISK_STORAGE_ALERT.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.en-US" has value "This is an alert from $productName The $datastore is used by the following Provider VDC(s): $pvdcsList"

VCD Email notification details:
name : DISK_STORAGE_ALERT
description : Alert when used disk storage exceeds threshold
config key : email.template.DISK_STORAGE_ALERT.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 following Provider VDC(s): $pvdcsList

Finding Orphaned VMs

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 vCloud Director database.
Virtual machines that are referenced in the vCenter database but not in the vCloud Director database are considered orphan VMs because vCloud 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 vCloud Director. His command has provisions for specifying an alternate trust store, which might be needed if you are working with vCloud Director or vCenter installations that use self-signed certificates.

Use a command with the following form:

```
cell-management-tool find-orphan-vms options
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--enableVerifyHostname</td>
<td>None</td>
<td>Enable the host name verification part of the SSL handshake.</td>
</tr>
<tr>
<td>--host</td>
<td>Required</td>
<td>IP address or fully-qualified domain name of the vCloud Director installation to search for orphan VMs.</td>
</tr>
<tr>
<td>--output-file</td>
<td>path name or -</td>
<td>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.</td>
</tr>
<tr>
<td>--password (-p)</td>
<td>Required</td>
<td>vCloud Director system administrator password.</td>
</tr>
<tr>
<td>--port</td>
<td>vCloud Director HTTPS port.</td>
<td>Specify this only if you do not want this command to use the default vCloud Director HTTPS port.</td>
</tr>
<tr>
<td>--trustStore</td>
<td>Full path name to a Java trust store file.</td>
<td>Specify this only if you do not want this command to use the default vCloud Director trust store file.</td>
</tr>
<tr>
<td>--trustStorePassword</td>
<td>Password to specified --trustStore</td>
<td>Required only if you use --trustStore to specify an alternate trust store file.</td>
</tr>
<tr>
<td>--trustStoreType</td>
<td>The type of the specified --trustStore (PKCS12, JCEKS, ...)</td>
<td>Required only if you use --trustStore to specify an alternate trust store file.</td>
</tr>
<tr>
<td>--user (-u)</td>
<td>Required</td>
<td>vCloud Director system administrator user name.</td>
</tr>
<tr>
<td>--vc-name</td>
<td>Required</td>
<td>Name of vCenter to search for orphan VMs.</td>
</tr>
</tbody>
</table>
Table 11-20. Cell Management Tool Options and Arguments, find-orphan-vms Subcommand (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vc-password</td>
<td>Required</td>
<td>vCenter administrator password.</td>
</tr>
<tr>
<td>--vc-user</td>
<td>Required</td>
<td>vCenter administrator user name.</td>
</tr>
</tbody>
</table>

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)
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

Use the configure-ceip command of the cell management tool to join or leave the VMware Customer Experience Improvement Program (CEIP).

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](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.

To join or leave the VMware Customer Experience Improvement Program, use a command line with the following form:

```
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 11-21. Cell Management Tool Options and Arguments, configure-ceip Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help (-h)</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>--disable</td>
<td>None</td>
<td>Leave the VMware Customer Experience Improvement Program</td>
</tr>
<tr>
<td>--enable</td>
<td>None</td>
<td>Join the VMware Customer Experience Improvement Program</td>
</tr>
<tr>
<td>--status</td>
<td>None</td>
<td>Display this product's current participation status in the VMware Customer Experience Improvement Program</td>
</tr>
</tbody>
</table>

Example: Leave the VMware Customer Experience Improvement Program

To leave the VMware Customer Experience Improvement Program use a command like this one:

```
[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 system's 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
```

Migrate to a PostgreSQL Database

You can migrate an existing vCloud Director database from Oracle or Microsoft SQL Server to PostgreSQL by using the dbmigrate subcommand of the cell management tool.

```
cell-management-tool dbmigrate options
```

**Important**  Hot migration is not supported. Before you begin a database migration, you must stop vCloud Director services. Open a console, shell, or terminal window on the cell platform and run the Linux command `service vmware-vcd stop`. For information about starting and stopping vCloud Director services, see *vCloud Director Installation and Upgrade Guide*. 
Table 11-22. Cell Management Tool Options and Arguments, \texttt{dbmigrate} Subcommand

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{--help} \texttt{(-h)}</td>
<td>None</td>
<td>Provides a summary of available commands in this category.</td>
</tr>
<tr>
<td>\texttt{--database-host} \texttt{(-dbhost)}</td>
<td>IP address or fully qualified domain name.</td>
<td>IP address or fully-qualified domain name of the target PostgreSQL database host.</td>
</tr>
<tr>
<td>\texttt{--database-name} \texttt{(-dbname)}</td>
<td>The name of the PostgreSQL database.</td>
<td>The name you chose when you created the target PostgreSQL database. Typically \texttt{vcloud}.</td>
</tr>
<tr>
<td>\texttt{--database-password} \texttt{(-dbpassword)}</td>
<td>Password for the PostgreSQL database user.</td>
<td>Database user password for the target PostgreSQL database.</td>
</tr>
<tr>
<td>\texttt{--database-port} \texttt{(-dbport)}</td>
<td>Port number used by the PostgreSQL database service on the database host.</td>
<td>Port number used by the PostgreSQL database service on the database host.</td>
</tr>
<tr>
<td>\texttt{--database-ssl}</td>
<td>true or false</td>
<td>Configures the target PostgreSQL database to require an SSL connection from vCloud Director.</td>
</tr>
<tr>
<td>\texttt{--database-user} \texttt{(-dbuser)}</td>
<td>Name of the PostgreSQL database user.</td>
<td>Database user name for the target PostgreSQL database.</td>
</tr>
<tr>
<td>\texttt{--private-key-path}</td>
<td>Absolute path of private key that has had its public key added to the authorized keys of other cells in the server group.</td>
<td>Reconfigures all cells in the server group to use the target PostgreSQL database after migration completes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important</strong> All cells must permit SSH connections from the superuser without a password.</td>
</tr>
<tr>
<td>\texttt{--verbose}</td>
<td>None</td>
<td>Sends all log output to the console as well as to the log files. Includes information that reports migration status for each table and the progress of the entire operation.</td>
</tr>
</tbody>
</table>

If you use the \texttt{--private-key-path} option, all cells must be configured to permit SSH connections from the superuser without a password. To perform a verification, for example, you can run the following Linux command:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```
This example sets your identity to vcloud, then makes an SSH connection to the cell at cell-ip as root but does not supply the root password. If the private key in private-key-path on the local cell is readable by user vcloud.vcloud and the corresponding public key is present in the authorized-keys file for the root user at cell-ip, the command succeeds.

**Note** The vcloud user, vcloud group, and vcloud.vcloud account are created by the vCloud Director installer for use as an identity with which vCloud Director processes run. The vcloud user has no password.

**Example: Migrate the vCloud Director Database to PostgreSQL and Update Database Connection Properties for All Cells**

The following command migrates the current vCloud Director database to a target PostgreSQL database installed on host psql.example.com. Because the --private-key-path option is included, after the migration finishes successfully, all cells in the server group are reconfigured to connect to the target database.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool dbmigrate \
  -dbhost psql.example.com -dbport 5432 -dbuser vcd-dba -dbname vcloud -dbpassword P@55w0rd \
  --private-key-path /vcloud/.ssh/id_rsa
  configuring the target database...
```

If not including the --private-key-path option, after the migration finishes, you can connect the cells to the target database by running the reconfigure-database subcommand on each cell in the server group. See **Example: Reconfigure a Cell After Migrating the vCloud Director Database to PostgreSQL**.