You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
6 Managing vSphere Resources 105
   Managing vSphere vCenter Servers 105
   Managing vSphere ESX/ESXi Hosts 108
   Managing vSphere Datastores 109
   Managing Stranded Items 110
   View Resource Pool Properties 111
   View Storage Policy Properties 111

7 Managing Organizations 113
   Enable or Disable an Organization 113
   Delete an Organization 113
   Add a Catalog to an Organization 114
   Editing Organization Properties 114
   Managing Organization Resources 118
   Managing Organization vApps and Virtual Machines 118

8 Managing System Administrators and Roles 123
   Add a System Administrator 123
   Import a System Administrator 124
   Enable or Disable a System Administrator 124
   Delete a System Administrator 124
   Edit System Administrator Profile and Contact Information 125
   Send an Email Notification to Users 125
   Delete a System Administrator Who Lost Access to the System 125
   Import a Group 125
   Delete an LDAP Group 126
   View Group Properties 126
   Roles and Rights 126

9 Managing System Settings 129
   Modify General System Settings 129
   General System Settings 129
   Editing System Email Settings 131
   Configuring Blocking Tasks and Notifications 132
   Configuring the System LDAP Settings 133
   Customize the vCloud Director Client UI 136
   Configuring Public Addresses 137
   Configure the Account Lockout Policy 139
   Configure vCloud Director to use vCenter Single Sign On 139

10 Monitoring vCloud Director 141
   Viewing Tasks and Events 141
   Monitor and Manage Blocking Tasks 143
   View Usage Information for a Provider Virtual Datacenter 143
   View Usage Information for an Organization Virtual Datacenter 143
   Using vCloud Director's JMX Service 144
   Viewing the vCloud Director Logs 144
   vCloud Director and Cost Reporting 145
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.
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** on page 9
  
  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** on page 12
  
  You can access the vCloud Director user interface by using a Web browser.

- **System Administrator Home Page** on page 12
  
  The Home tab provides links to common tasks and support resources.

- **Preparing the System** on page 12
  
  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** on page 13
  
  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** on page 14
  
  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.

**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, port groups,
or Cloud isolated networks. 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,” on page 15</td>
</tr>
<tr>
<td>Create a Provider Virtual Datacenter</td>
<td>“Create a Provider Virtual Datacenter,” on page 17</td>
</tr>
<tr>
<td>Create an External Network</td>
<td>“Add an External Network,” on page 19</td>
</tr>
<tr>
<td>Create a Network Pool</td>
<td>“Network Pools,” on page 19</td>
</tr>
<tr>
<td>Create an Organization</td>
<td>“Create an Organization,” on page 25</td>
</tr>
<tr>
<td>Allocate Resources to an Organization</td>
<td>“Create an Organization Virtual Datacenter,” on page 52</td>
</tr>
</tbody>
</table>
Table 1-1. Quick Start Tasks (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Network to an Organization</td>
<td>“Adding Networks to an Organization Virtual Datacenter,” on page 83</td>
</tr>
<tr>
<td>Add a Catalog to an Organization</td>
<td>“Add a Catalog to an Organization,” on page 114</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 vCloud Director configuration script to upgrade the SSL certificates on a vCloud Director server. When you run this script on a server that has already been configured, it validates the database connection details and prompts for SSL certificate information, but skips all the other configuration steps, so that the existing configuration is not modified.

Each vCloud Director server requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. You must execute this procedure 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.

Prerequisites

This procedure requires you to stop vCloud Director services on each server for which you replace certificates. Stopping a server can have an impact on cloud operations.

- Have the following information available:
  - Location and password of the keystore file that includes the SSL certificates for this server. See the vCloud Director Installation and Configuration Guide. The configuration script does not run with a privileged identity, so the keystore file and the directory in which it is stored must be readable by any user.
  - Password for each SSL certificate.

Procedure

1. Log in to the target server as root.
2. Stop vCloud Director services on the server.
3. Run the configuration script on the server.
   - Open a console, shell, or terminal window, and type:
     `/opt/vmware/vcloud-director/bin/configure`
4. Specify the full path to the Java keystore file that holds the new certificates.
   - Please enter the path to the Java keystore containing your SSL certificates and private keys:/opt/keystore/certificates.ks
5. Enter the keystore and certificate passwords.
   - Please enter the password for the keystore:
   - Please enter the private key password for the 'http' SSL certificate:
   - Please enter the private key password for the 'consoleproxy' SSL certificate:

The configuration script replaces the certificates and re-starts vCloud Director services on the server.
What to do next
If you have acquired new certificates for any other members of the vCloud Director server group, use this procedure to replace the existing certificates on those servers

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.
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,” on page 15
- “Adding Cloud Resources,” on page 17

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 ESX/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 vShield 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 on page 16
   - 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 on page 16
   - To attach a vCenter Server to vCloud Director, you must provide connection information and a display name for the vCenter Server.

3. Connect to vShield on page 16
   - vCloud Director requires vShield to provide network services. Each vCenter Server you attach to vCloud Director requires its own instance of vShield.

4. Confirm Settings and Attach the vCenter Server on page 16
   - 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 vShield

vCloud Director requires vShield to provide network services. Each vCenter Server you attach to vCloud Director requires its own instance of vShield.

Procedure
1. Type the host name or IP address of the vShield instance to use with the vCenter Server that you are attaching.
2. Type the user name and password to connect to vShield.
   The default user name is admin and the default password is default. You can change these defaults in the vShield 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 vShield.
2. (Optional) Click Back to modify the settings.
3. Click Finish to accept the settings and attach the vCenter Server.
vCloud Director attaches the new vCenter Server and registers its resources for provider virtual datacenters to use.

**What to do next**
Assign a vShield for VMware vCloud Director license key in the vCenter Server.

**Assign a vShield License Key in vCenter**
After you attach a vCenter Server to vCloud Director, you must use the vSphere Client to assign a vShield for VMware vCloud Director license key.

**Prerequisites**
The vSphere Client must be connected to the vCenter Server system.

**Procedure**
1. From a vSphere Client host that is connected to the vCenter Server system, select **Home > Licensing.**
2. For the report view, select **Asset.**
3. Right-click the vShield Edge 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 vShield for VMware vCloud Director 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,” on page 30.

For more information about organization virtual datacenter networks, see “Managing Organization Virtual Datacenter Networks,” on page 82

**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 connected to that resource pool.

A provider virtual datacenter is the source for organization virtual datacenters.

**Create a Provider Virtual Datacenter**
You can create a provider virtual datacenter to register vSphere compute, memory, and storage resources for vCloud Director to use. You can create multiple provider virtual datacenters for users in different geographic locations or business units, or for users with different performance requirements.

A provider virtual datacenter can include only a single resource pool from a single vCenter Server.
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.

**Prerequisites**

- Verify that at least one vCenter Server is attached with an available resource pool to vCloud Director. The resource pool must be in a vCenter cluster configured to use automated DRS. The vCenter Server must have the vShield for VMware vCloud Director license key.
- Verify that vSAN is disabled on the vSphere cluster you are using.
- Set up the VXLAN infrastructure in vShield Manager. See “VXLAN Virtual Wires Management” in the vShield Administration Guide.

**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. You can use the name and description fields to indicate the vSphere functions available to the provider virtual datacenter, for example, vSphere HA.
4. Select the latest supported hardware version and click Next.
   This selection determines the latest supported hardware version for virtual machines in organization virtual datacenters based on this provider virtual datacenter. Hardware Version 10 requires ESXi 5.5 hosts.
5. Select a vCenter Server and resource pool and click Next.
   If the vCenter Server has no available resource pools, no resource pools appear in the list.
6. Select one or more storage policies for the provider virtual datacenter to support, click Add, and click Next.
7. Click Finish to create the provider virtual datacenter.
   vCloud Director creates a provider virtual datacenter and associated VXLAN network pool.

**What to do next**

You can enable vSAN on the cluster after the provider virtual datacenter has been created.

**External Networks**

An external network is a logical, differentiated network based on a vSphere port group. An external network provides the interface to the Internet for virtual machines connected to external organization virtual datacenter networks.

For more information about organization virtual datacenter networks, see “Managing Organization Virtual Datacenter Networks,” on page 82.
Add an External Network

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

Prerequisites

A vSphere port group is available. If the port group uses VLAN, it can use only a single VLAN. Port groups with VLAN trunking are not supported.

VMware recommends using an auto-expanding static port group.

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 a vSphere port group and click Next.
4. Type the network settings and click Next.
5. Type a name and optional description for the network and click Next.
6. 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, port groups, or cloud isolated networks. 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

vSphere VXLAN networks are based on the IETF draft VXLAN standard. These networks support the local-domain isolation equivalent to what is vSphere isolation-backed networks support.

When you create a provider virtual datacenter, a VXLAN network pool is created in vCloud Director. When you use this network pool, VXLAN virtual wires are created in vCenter Server. Most configurations do not require network pools beyond the 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. You cannot create a VXLAN network pool by any other method. If you rename a provider virtual datacenter, its VXLAN network pool is automatically renamed.
vSphere VXLAN networks 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 in a vCloud environment, see the vShield Administration Guide.

**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 ESX/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 the layer 2 level. The port groups must be physically isolated or must be isolated by using VLAN tags. Failure to properly isolate the port groups can cause a disruption on the network.
Prerequisites
Verify that one or more port groups are available in vSphere. The port groups must be available on each ESX/ESXi host in the cluster, and each port group must use only a single VLAN. Port groups with VLAN trunking are not 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.

Add a Network Pool That Is Backed by Cloud Isolated Networks
You can create a network pool that is backed by cloud isolated networks. A cloud isolated network spans hosts, provides traffic isolation from other networks, and is the best source for vApp networks.
An isolation-backed network pool does not require preexisting port groups in vSphere.

Prerequisites
Verify that a vSphere distributed switch is available.

Procedure
1. Click the Manage & Monitor tab and click Network Pools in the left pane.
2. Click Add Network Pool.
3. Select VCD Network Isolation-backed and click Next.
4. Type the number of networks to create from the network pool.
5. (Optional) Type a VLAN ID.
6. Select a vCenter Server and a vSphere distributed switch and click Next.
7. Type a name and optional description for the network and click Next.
8. Review the network pool settings and click Finish.

vCloud Director creates cloud isolated networks in vSphere as they are needed.

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. You can also increase the network pool MTU. See “Set the MTU for a Network Pool Backed by Cloud Isolated Networks,” on page 22.
Set the MTU for a Network Pool Backed by Cloud Isolated Networks

You can specify the maximum transmission units (MTU) that vCloud Director uses for a network pool that is backed by Cloud isolated networks. The MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets.

When you configure the virtual machine guest operating system and the underlying physical infrastructure with the standard MTU (1500 bytes), the VMware network isolation protocol fragments frames. To avoid frame fragmentation, increase the MTU to at least 1600 bytes for the network pool and the underlying physical network. You can increase the network pool MTU up to, but not greater than, the MTU of the physical network.

If your physical network has an MTU of less than 1500 bytes, decrease the MTU of the network pool to match the underlying physical network.

Prerequisites

Verify that you have a network pool backed by cloud isolated networks. Before you increase the MTU for a network pool, you must ensure that the physical switch infrastructure supports an MTU of greater than 1500, also known as jumbo frames.

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 MTU tab, type the MTU and click OK.

vCloud Director modifies the MTU for the network pool and all other network pools that use the same vSphere distributed switch.
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,” on page 23
- “Understanding Allocation Models,” on page 24
- “Create an Organization,” on page 25
- “Allocate Resources to an Organization,” on page 30

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,” on page 29.

Users can configure email notification to receive a message before a runtime or storage lease expires. See “Set User Preferences,” on page 14 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,” on page 129.

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 vCPUs 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** on page 26
   - Open the New Organization wizard to start the process of creating an organization.
2 Name the Organization on page 26
Provide a descriptive name and an optional description for your new organization.

3 Specify the Organization LDAP Options on page 27
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 on page 27
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 on page 28
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 on page 28
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 on page 29
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 on page 29
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 the System LDAP Settings,” on page 133.

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.

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</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>organizations</td>
<td></td>
</tr>
<tr>
<td>Allow creation of catalog feeds for</td>
<td>Allows organization administrators to share this organization’s catalogs with organizations outside this instance of vCloud Director.</td>
</tr>
<tr>
<td>consumption by external organizations</td>
<td></td>
</tr>
<tr>
<td>Allow subscription to external</td>
<td>Allows organization administrators to subscribe this organization to catalog feeds from outside this instance of vCloud Director.</td>
</tr>
<tr>
<td>catalog feeds</td>
<td></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</td>
<td>The organization uses the system notification settings.</td>
</tr>
<tr>
<td>settings</td>
<td></td>
</tr>
<tr>
<td>Set organization notification</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>
<tr>
<td>settings</td>
<td></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,” on page 23.

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 on page 31
   Open the Allocate Resources wizard to start the process of creating an organization virtual datacenter for an organization.

2. Select a Provider Virtual Datacenter on page 31
   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 on page 31
   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 on page 32
   Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

5. Allocate Storage on page 33
   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. Select Network Pool and Services on page 34
   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 on page 34
   You configure an edge gateway to provide connectivity to one or more external networks.

8. Configure External Networks on page 35
   Select the external networks that the edge gateway can connect to.

9. Configure IP Settings on a New Edge Gateway on page 35
   Configure IP settings for external networks on the new edge gateway.

10. Suballocate IP Pools on a New Edge Gateway on page 35
    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 on page 35
    Configure the inbound and outbound rate limits for each external network on the edge gateway.

12. Create an Organization Virtual Datacenter Network on page 36
    You can create an organization virtual datacenter network that is connected to the new edge gateway.

13. Name the Organization Virtual Datacenter on page 36
    You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new 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,” on page 24.

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 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 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>
<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 avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk’s current and future activities. ESX/ESXi commits only as much storage space as the disk needs for its initial operations.
Fast provisioning saves time by using vSphere linked clones for certain operations. See “Fast Provisioning of Virtual Machines,” on page 120.

**IMPORTANT** Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider virtual datacenter on which the organization virtual datacenter is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider virtual datacenter on which the organization virtual datacenter is based contains any VMFS datastores connected to more than 8 hosts, powering on virtual machines might fail. Make sure that datastores are connected to a maximum of 8 hosts.

**Procedure**

1. Select the storage policy to allocate and click **Add**.
2. Enter the amount of storage to allocate.
3. Select the **Default instantiation profile** 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**.

**Select 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. Enter the maximum number of networks that the organization can provision from the network pool.
3. (Optional) Select **Enable** for each available third-party or edge gateway service to enable.
4. Click **Next**.

**Configure an Edge Gateway**

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

**Procedure**

1. (Optional) Select **Create a new edge gateway** to create and configure an edge gateway.
2. Type a name and optional description for the new Edge gateway.
3. Select a gateway configuration for the edge gateway.
4. Select **Enable High Availability** to enable high availability on the edge gateway.
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.
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.
2 (Optional) Deselect **Enabled**.
   Disabling the organization virtual datacenter prevents new vApps from being deployed to the virtual datacenter.
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.
You can create a catalog to make a set of vApp templates or media files available to organizations in a single vCloud Director installation or to organizations across multiple vCloud Director installations.

Organizations use catalogs to store vApp templates and media files. The members of an organization can use catalog items as the building blocks to create their own vApps.

When you share a catalog, the items in the catalog become available to all or selected organizations in the vCloud Director installation. The administrators of each organization can then choose which catalog items to provide to their users.

When you publish a catalog for external organizations to use, the items in the catalog become available to organizations across multiple vCloud Director installations. For an organization outside the vCloud Director installation to access an externally published catalog, the organization must subscribe to the catalog.

Before you can create a published catalog, you must create and provision an organization to contain the catalog.

This chapter includes the following topics:

- “Enable Catalog Sharing, Publishing, and Subscription,” on page 37
- “Create a Catalog,” on page 38
- “Upload a vApp Template,” on page 39
- “Import a vApp Template from vSphere,” on page 40
- “Upload a Media File,” on page 40
- “Import a Media File from vSphere,” on page 41
- “Share a Catalog,” on page 41
- “Publish a Catalog to External Organizations,” on page 42
- “Subscribe to an External Catalog Feed,” on page 42

Enable Catalog Sharing, Publishing, and Subscription

Before you can share or publish an organization's catalogs, you must enable catalog sharing or publishing for the organization. Before you can subscribe to external organization's catalogs, you must enable subscription to external catalogs.

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 Catalog.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow sharing catalogs to other organizations</strong></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><strong>Allow creation of catalog feeds for consumption by external organizations</strong></td>
<td>Allows organization administrators to share this organization’s catalogs with organizations outside this instance of vCloud Director.</td>
</tr>
<tr>
<td><strong>Allow subscription to external catalog feeds</strong></td>
<td>Allows organization administrators to subscribe this organization to catalog feeds from outside this instance of vCloud Director.</td>
</tr>
</tbody>
</table>

### Create a Catalog

You can create a catalog to contain uploaded and imported vApp templates, media files, and other files to make available to all organizations. An organization can have multiple catalogs and control access to each catalog individually.

**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 and select My Organization’s Catalogs in the left pane.
4. On the Catalogs tab, click Add Catalog.
5. Type a catalog name and optional description and click Next.
6. 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><strong>Use any available storage in the organization</strong></td>
<td>This catalog uses any available storage in the organization.</td>
</tr>
<tr>
<td><strong>Pre-provision storage on specific storage policy</strong></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>

7 Click Add Members.

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 select users or groups to which to grant catalog access.

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 users to add vApp templates and ISOs to the catalog.
   - Select Full Control to grant full control of the catalog’s contents and settings.
8 Click **Add Organizations**.
   a Select which organizations on this vCloud Director installation can access this catalog.

   Select **All organizations** to allow all organizations in the vCloud Director installation to have access to this catalog.

   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 users to add vApp templates and ISOs to the catalog.
   - Select **Full Control** to grant full control of the catalog’s contents and settings.

9 Click **Next**.

10 (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.

11 (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.

12 (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.

13 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.

---

**Upload a vApp Template**

You can upload an OVF package as a vApp template to make the template available to other users. vCloud Director supports Open Virtualization Format (OVF) 1.0 and OVF 1.1.

vCloud Director supports OVF based on the OVF Specification. If you upload an OVF package that includes deployment options, those options are preserved in the vApp template.

**Prerequisites**

Verify that the following conditions exist:

- The organization to which you are uploading the OVF package has a catalog and an organization virtual datacenter.
- The computer from which you are uploading has Java Plug-in 1.6.0_10 or later installed.

**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 **Catalog** and select **My Organization’s Catalogs** in the left pane.

4 On the **vApp Templates** tab, click **Upload**.

5 Click **Browse**, browse to the location of the OVF package, select it, and click **Open**.

6 Type a name and optional description for the vApp template.

7 Select a catalog and click **Upload**.
What to do next
Make sure that vSphere Tools is installed on the virtual machines in the vApp. vSphere Tools is required to support guest customization. See the VMware vCloud Director User’s Guide.

Import a vApp Template from vSphere
You can import a virtual machine from vSphere and save it as a vApp template in a catalog that is available to other users.

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 Catalog and select My Organization’s Catalogs in the left pane.
4. On the vApp Templates tab, click Import from vSphere.
5. Select a vCenter Server and a virtual machine.
6. Type a name and optional description for the vApp template.
7. Select a catalog.
8. Choose whether to move or copy the virtual machine to the catalog.
9. Choose whether to designate the vApp template as a Gold Master in the catalog.
   If you mark a vApp template as a Gold Master, this information appears in the list of vApp templates.
10. Click OK.

What to do next
Check that vSphere Tools is installed on the virtual machines in the vApp. vSphere Tools is required to support guest customization. See the VMware vCloud Director User’s Guide.

Upload a Media File
You can upload an ISO or FLP file to make the media available to other users.

Prerequisites
Verify that the computer from which you are uploading has Java Plug-in 1.6.0_10 or later installed.

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 Catalog and select My Organization’s Catalogs in the left pane.
4. On the Media tab, click Upload.
5. Click Browse, browse to the location of the media file, select it, and click Open.
6. Type a name and optional description for the media file.
   The file name must contain an extension, such as .iso.
7. Select a catalog and click Upload.
Import a Media File from vSphere

You can import a media file from a vSphere datastore and save it in a catalog available to other users.

**Prerequisites**

You must be a vCloud Director system administrator. You must know which datastore contains the media file and the path to that file.

**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 Catalog and select My Organization's Catalogs in the left pane.
4. On the Media tab, click the Import from vSphere button.
5. Type a name and optional description for the media file.
6. Select the source vCenter Server and datastore and type the path to the media file.
7. Select a catalog.
8. Click OK.

Share a Catalog

You can share a catalog to make its vApp templates and media files available to all organizations in the vCloud Director installation.

**Prerequisites**

Verify that the organization that contains the catalog allows catalog sharing.

**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 Catalog and select My Organization's Catalogs in the left pane.
4. On the Catalogs tab, right-click the catalog name and select Publish Settings.
5. On the Sharing tab, click Add Members.
6. 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>Everyone in this organization</td>
<td>All users and groups in the organization have access to this catalog.</td>
</tr>
<tr>
<td>Specific users and groups</td>
<td>Select users or groups to grant catalog access to and click Add.</td>
</tr>
</tbody>
</table>
7 Select the access level for users with access to this catalog from the drop-down menu and click **OK**.

<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>

8 Click **Add Organizations**.

9 Select which organizations on this vCloud Director installation can access this catalog.

<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.</td>
</tr>
<tr>
<td>Specific organizations</td>
<td>Select the organizations to grant catalog access to and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

10 Click **OK** and click **OK** again.

The catalog and all of its contents appear under Public Catalogs for selected users, groups, and organizations in the vCloud Director installation.

### Publish a Catalog to External Organizations

You can publish a catalog externally to make its vApp templates and media files available to all organizations outside the vCloud Director installation.

**Prerequisites**

Verify that the organization that contains the catalog allows external catalog publishing.

**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 **Catalog** and select **My Organization’s Catalogs** in the left pane.
4 On the **Catalogs** tab, right-click the catalog name and select **Publish Settings**.
5 On the **External Publishing** tab, select **Enabled** and supply a password for the catalog feed.
6 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.

### Subscribe to an External Catalog Feed

You subscribe an organization to an external catalog feed to access a catalog from outside the installation of vCloud Director.

**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** and select **My Organization’s Catalogs** in the left pane.

4 Click **Add Catalog** and type a name and optional description for the catalog feed.

5 Select **Subscribe to an external catalog** and click **Next**.

6 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><strong>Use any available storage in the organization</strong></td>
<td>This catalog feed uses any available storage in the organization.</td>
</tr>
<tr>
<td><strong>Pre-provision storage on specific storage policy</strong></td>
<td>Select a virtual datacenter storage policy to use for this catalog feed and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

7 Click **Add Members**.

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

9 Click **Add Organizations**.

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

11 Click **Next**.

12 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,” on page 45
- “Managing Organization Virtual Datacenters,” on page 52
- “Managing External Networks,” on page 63
- “Managing Edge Gateways,” on page 65
- “Managing Organization Virtual Datacenter Networks,” on page 82
- “Managing Network Pools,” on page 96
- “Managing Cloud Cells,” on page 98
- “Managing Service Offerings,” on page 99

Managing Provider Virtual Datacenters

After you create a provider virtual datacenter, you can modify its properties, disable or delete it, and manage its ESX/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.
4. (Optional) Enter a new name and description for the provider virtual datacenter.
5. Click OK.

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

Enable or Disable a Provider Virtual Datacenter 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 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.

vCloud Director enables or disables the host for all provider virtual datacenters that use its resources.

Prepare or Unprepare a Provider Virtual Datacenter Host

When you add an ESX/ESXi host to a vSphere cluster that vCloud Director uses, you must prepare the host before a provider virtual datacenter can use its resources. You can unprepare a host to remove it from the vCloud Director environment.

For information about moving running virtual machines from one host to another, see “Move Virtual Machines from one ESX/ESXi Host to Another,” on page 108.

You cannot prepare a host that is in lockdown mode. After you prepare a host, you can enable lockdown mode.

Prerequisites

Before you can unprepare a host, you must disable it and ensure that no virtual machines are running on the host.

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 Prepare Host or Unprepare Host.

vCloud Director prepares or unprepares the host for all provider virtual datacenters that use its resources.

Upgrade an ESX/ESXi Host Agent for a Provider Virtual Datacenter Host

vCloud Director installs agent software on each ESX/ESXi host in the installation. If you upgrade your ESX/ESXi hosts, you also need to upgrade your ESX/ESXi host agents.

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 Upgrade Host.

vCloud Director upgrades the host agent. This upgrade affects all provider virtual datacenters that use the host.

Repair a Provider Virtual Datacenter ESX/ESXi Host

If the vCloud Director agent on an ESX/ESXi host cannot be contacted, try to repair the host.

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 Repair Host.

vCloud Director repairs the host. This operation affects all provider virtual datacenters that use the host.

**Enable vSphere VXLAN on an Upgraded Provider Virtual Datacenter**

Enable vSphere VXLAN on an upgraded provider virtual datacenter to create a VXLAN network pool for the provider virtual datacenter.

vSphere VXLAN is enabled by default for new provider virtual datacenters.

**Prerequisites**

Configure VXLAN for your vCloud environment. See the *vShield Administrator’s Guide*.

**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 VXLAN.

A VXLAN network pool is created for the provider virtual datacenter. See “VXLAN Network Pools,” on page 19.

**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>
<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 Storage Policy to a Provider Virtual Datacenter

Add a storage policy to a provider virtual datacenter to support the storage policy for organization virtual datacenters backed by the provider virtual datacenter.

Storage policies are created and managed in vSphere. See the vSphere documentation or contact your vSphere administrator.

**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. Click **Add Storage Policy**.
5. 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 provider virtual datacenter’s clusters.
6. Click **OK**.

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

**What to do next**

Configure organization virtual datacenters backed by the provider virtual datacenter to support the storage policy. See “Add a Storage Policy to an Organization Virtual Datacenter,” on page 62.

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 Virtual Datacenter

You can add additional resource pools to a provider virtual datacenter 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.

**Prerequisites**

Verify that one or more available resource pool exists in the same vCenter datacenter as the provider virtual datacenter'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.
4 Click Add Resource Pool.
5 Select the resource pool to add and click Finish.

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 vShield virtual machines and virtual machines 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 on page 53

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 on page 54
   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 on page 54
   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 on page 54
   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 on page 55
   Configure the allocation model to specify the amount of provider virtual datacenter resources to allocate to the organization virtual datacenter.

6 Allocate Storage on page 56
   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 Select Network Pool and Services on page 57
   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 on page 57
   You configure an edge gateway to provide connectivity to one or more external networks.

9 Configure External Networks on page 58
   Select the external networks that the edge gateway can connect to.

10 Configure IP Settings on a New Edge Gateway on page 58
    Configure IP settings for external networks on the new edge gateway.

11 Suballocate IP Pools on a New Edge Gateway on page 58
    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 on page 58
    Configure the inbound and outbound rate limits for each external network on the edge gateway.

13 Create an Organization Virtual Datacenter Network on page 59
    You can create an organization virtual datacenter network that is connected to the new edge gateway.

14 Name the Organization Virtual Datacenter on page 59
    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 on page 59
    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,” on page 24.

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 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 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 5.2. 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>
<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 avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk’s current and future activities. ESX/ESXi commits only as much storage space as the disk needs for its initial operations.
Fast provisioning saves time by using vSphere linked clones for certain operations. See “Fast Provisioning of Virtual Machines,” on page 120.

**IMPORTANT** Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider virtual datacenter on which the organization virtual datacenter is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider virtual datacenter on which the organization virtual datacenter is based contains any VMFS datastores connected to more than 8 hosts, powering on virtual machines might fail. Make sure that datastores are connected to a maximum of 8 hosts.

**Procedure**

1. Select the storage policy to allocate and click Add.
2. Enter the amount of storage to allocate.
3. Select the Default instantiation profile 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.

**Select 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. Enter the maximum number of networks that the organization can provision from the network pool.
3. (Optional) Select Enable for each available third-party or edge gateway service to enable.
4. Click Next.

**Configure an Edge Gateway**

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

**Procedure**

1. (Optional) Select Create a new edge gateway to create and configure an edge gateway.
2. Type a name and optional description for the new Edge gateway.
3. Select a gateway configuration for the edge gateway.
4. Select Enable High Availability to enable high availability on the edge gateway.
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.
2. (Optional) Deselect **Enabled**.
   - Disabling the organization virtual datacenter prevents new vApps from being deployed to the virtual datacenter.
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.
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.

- Modify an Organization Virtual Datacenter Name and Description on page 60
  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 on page 61
  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 on page 61
  After you create and use an organization virtual datacenter, you might decide to provide it with more storage resources from its source 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 on page 62
  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 Poll 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 Poll 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 might decide to provide it with more
storage resources from its source provider virtual datacenter. You can also enable or disable thin
provisioning and fast provisioning for the organization virtual datacenter.

Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider virtual
datacenter on which the organization virtual datacenter is based contains ESX/ESXi 4.x hosts, you must
disable fast provisioning. For information about fast provisioning, see “Fast Provisioning of Virtual
Machines,” on page 120.

**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 Storage Policy to a Provider Virtual Datacenter,” on page 49.

**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 External Networks

After you create an external network, you can modify its name, description, and network specification, add IP addresses to its IP address pool, or delete the network.

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 on page 63
  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 on page 64
  If the network specification for an external network changes, you can modify its network settings.
- Delete and External Network Specification on page 64
  You can delete an external network specification that is no longer in use.

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.
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.
4. 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.

Delete and External Network Specification

You can delete an external network specification that is no longer in use.

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 delete, and click Delete.
4. 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 vShield. For more information, see the vShield 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** on page 65
   Open the New Edge Gateway wizard to start the process of adding an edge gateway to an
   organization virtual datacenter.

2. **Select Gateway and IP Configuration Options for a New Edge Gateway** on page 66
   Configure the edge gateway to connect to one or more physical networks.

3. **Select External Networks for a New Edge Gateway** on page 66
   Select the external networks that the edge gateway can connect to.

4. **Configure IP Settings on a New Edge Gateway** on page 66
   Configure IP settings for external networks on the new edge gateway.

5. **Suballocate IP Pools on a New Edge Gateway** on page 66
   Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway
   provide.

6. **Configure Rate Limits on a New Edge Gateway** on page 67
   Configure the inbound and outbound rate limits for each external network on the edge gateway.

7. **Configure the Name and Description of a New Edge Gateway** on page 67
   Enter a name and optional description for the edge gateway.

8. **Review the Configuration of a New Edge Gateway** on page 67
   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 a gateway 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>Full</td>
<td>Provides increased capacity and performance. Full and Full-4 configurations provide identical security functions.</td>
</tr>
<tr>
<td>Full-4</td>
<td>Provides increased capacity and performance. Full and Full-4 configurations provide identical security functions. ESXi must have at least 8 vCPU available to deploy a Full-4 edge gateway with high availability enabled.</td>
</tr>
</tbody>
</table>

2. (Optional) Select Enable High Availability to enable high availability on the edge gateway.

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

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

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

6. 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**.
Configuring Edge Gateway Services

You can configure services, such as DHCP, firewalls, network address translation (NAT), and VPN for edge gateways. Organization administrators can also configure some network services for their edge gateways.

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,” on page 70

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,” on page 69.

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,” on page 71.

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 can 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.

Both system administrators and organization administrators can create VPN tunnels.

If there is a firewall 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 in each of the organizations. The organization virtual datacenter networks must have non-overlapping IP subnets and site-to-site 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 another organization from the drop-down menu.
7. Click Connect to another organization, type the login information for the peer organization, and click Continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud URL</td>
<td>The base URL of the vCloud instance that contains the peer organization. For example, <a href="https://www.example.com">https://www.example.com</a>. Do not include /cloud or /cloud/org/orgname in the URL.</td>
</tr>
<tr>
<td>Organization</td>
<td>The organization name that is used as the unique identifier in the organization URL. For example, if the organization URL is <a href="https://www.example.com/cloud/org/myOrg">https://www.example.com/cloud/org/myOrg</a>, type myOrg.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name of an organization administrator or system administrator that has access to the organization.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
</tbody>
</table>

8. Select a peer network.
9. Review the tunnel settings and click Connect.

vCloud Director configures both peer network endpoints.
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,” on page 74.

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,” on page 74.

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,” on page 72.

**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**.

### Enable Static Routing on an Edge Gateway

You can configure an edge gateway to provide static routing services. After you enable static routing on an edge gateway, you can add static routes to allow traffic between vApp networks routed to organization virtual datacenter networks backed by the 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 **Static Routing** tab, select **Enable static routing**, and click **OK**.

**What to do next**

Create static routes. See “Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network,” on page 90 and “Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks,” on page 92.

### 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 on page 76
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 on page 77
You can edit the settings of an existing pool server.

Delete a Pool Server on page 78
You can delete a pool server from an edge gateway.

Add a Virtual Server to an Edge Gateway on page 78
A virtual server is a highly scalable and highly available server built on a cluster of servers called members.

Edit Virtual Server Settings on page 78
You can edit the settings of an existing virtual server.

Delete a Virtual Server on page 79
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.
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,” on page 76.

**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. 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.
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,” on page 76.

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,” on page 78.
**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** on page 79
  You can configure an edge gateway for high availability.

- **Configure External Networks on an Edge Gateway** on page 80
  Add or remove external networks connected to an edge gateway.

- **Configure External Network IP Settings on an Edge Gateway** on page 80
  Change the IP address for external interfaces on an edge gateway.

- **Suballocate IP Pools on an Edge Gateway** on page 80
  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** on page 81
  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.

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 **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.
3 Click the Edge Gateways tab, right-click the edge gateway name, and select Synchronize syslog server settings.
4 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 on page 83
  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.

- Configuring Organization Virtual Datacenter Network Services on page 85
  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 on page 93
  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 on page 94
  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.
- **Delete an Organization Virtual Datacenter Network** on page 94

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** on page 94

You can view a list of IP addresses that are currently in use in an organization virtual datacenter network IP pool.

- **Editing Organization Virtual Datacenter Network Properties** on page 95

You can edit the properties of an existing organization virtual datacenter network, including the network name and description, IP addresses, and DNS settings.

### 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>
<thead>
<tr>
<th>Organization Virtual Datacenter Network Type</th>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>External organization virtual datacenter network - direct connection</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>External network</td>
</tr>
<tr>
<td>External organization virtual datacenter network - NAT-routed connection</td>
<td>Accessible only by this organization. Only virtual machines within this organization can connect to this network. This network also provides controlled access to an external network. System administrators and organization administrators can configure network address translation (NAT) and firewall settings to make specific virtual machines accessible from the external network. On the <strong>Org VDC Networks</strong> tab, NAT-routed networks display a gateway address.</td>
<td>vSphere Edge 5.1 and an edge gateway</td>
</tr>
<tr>
<td>Internal 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. Machines outside of this organization have no connectivity to machines within the organization. On the <strong>Org VDC Networks</strong> tab, internal networks do not display an associated gateway address.</td>
<td>Network pool</td>
</tr>
</tbody>
</table>
Create an External Direct Organization Virtual Datacenter Network

You can create an external direct organization virtual datacenter network that multiple organizations can access. You typically use the external network to connect to the Internet. The organization connects directly to this network.

Prerequisites

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 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 organization virtual datacenter network available to other organization virtual datacenters in the organization.
8. Click Next.
9. Review the settings for the organization virtual datacenter network.
   - Click Finish to accept the settings and create the organization virtual datacenter network, or click Back to modify the settings.

Create an External Routed Organization Virtual Datacenter Network

You can create an external routed organization virtual datacenter network that only this organization can access.

Prerequisites

Verify that you have an edge gateway on your 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 Org VDC Networks tab and click Add Network.
4. Select Create a routed network by connecting to an existing edge gateway.
5. Select an edge gateway and click Next.
6. Type a Gateway address and Network mask for the organization virtual datacenter network.
7. (Optional) Select Use gateway DNS to use the DNS relay of gateway.
   - This option is available only if the gateway has DNS relay enabled.
8. (Optional) Enter DNS settings to use DNS.
9. (Optional) 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.
10. Click Next.
11. Type a name and optional description.

12. (Optional) Select **Share this network with other VDCs in the organization** to make the organization virtual datacenter network available to other organization virtual datacenters in the organization.

13. Click **Next**.

14. Review the settings for the organization virtual datacenter network.

   Click **Finish** to accept the settings and create the organization virtual datacenter network, or click **Back** to modify the settings.

### Create an Internal Organization Virtual Datacenter Network

You can create an internal organization virtual datacenter network that only this organization can access. The new network provides the organization with an internal network to which multiple vApps can connect.

**Prerequisites**

Verify that you have a network 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 and click **Add Network**.

4. Select **Create an isolated network within this virtual datacenter** and click **Next**.

5. Type a **Gateway address** and **Network mask** for the organization virtual datacenter network.

6. (Optional) Select **Use gateway DNS** to use the DNS relay of gateway.

   This option is available only if the gateway has DNS relay enabled.

7. (Optional) Enter DNS settings to use DNS.

8. (Optional) 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.

9. Click **Next**.

10. Type a name and optional description.

11. (Optional) Select **Share this network with other VDCs in the organization** to make the organization virtual datacenter network available to other organization virtual datacenters in the organization.

12. Click **Next**.

13. Review the settings and click **Finish** to accept the settings.

   An organization virtual datacenter network is created.

### 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 5-7** lists the network services that vCloud Director provides to each type of organization virtual datacenter network.
Table 5-7. 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,” on page 87.

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,” on page 86.

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,” on page 88.

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.
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 click Add.
5. Type a name for the rule.
6. Select the traffic direction.
7. 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.
8. 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.
9. Select the protocol and action.
   - A firewall rule can allow or deny traffic that matches the rule.
10. Select the Enabled check box.
11 (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.

12 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.

6 Click OK.

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.

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.

### Enable Static Routing for an Organization Virtual Datacenter Network

You can configure certain organization virtual datacenter networks to provide static routing services. After you enable static routing on an organization virtual datacenter network, you can add static routes to allow traffic between different vApp networks routed to the organization virtual datacenter network.

**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**.

4 On the **Static Routing** tab, select **Enable static routing** and click **OK**.

**What to do next**

Create static routes. See “Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network,” on page 90 and “Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks,” on page 92.

### 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
Verify that the networks have the following configurations:
- vShield is installed.
- 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 5-8. Network Information

<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 5-9. 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,” on page 87.
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**.
4. On the **Static Routing** tab, click **Add**.
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>
<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,” on page 87.

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,” on page 94.

**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**.
Editing Organization Virtual Datacenter Network Properties

You can edit the properties of an existing organization virtual datacenter network, including the network name and description, IP addresses, and DNS settings.

- **Add IP Addresses to an Organization Virtual Datacenter Network IP Pool** on page 95
  
  If an organization virtual datacenter network is running out of IP addresses, you can add more addresses to its IP Pool.

- **Modify an Organization Virtual Datacenter Network Name and Description** on page 95
  
  As your vCloud Director installation increases, you might want to assign a more descriptive name or description to an existing organization virtual datacenter network.

- **Modify an Organization Virtual Datacenter Network DNS Settings** on page 96
  
  You can change the DNS settings for certain types of organization virtual datacenter networks.

Add IP Addresses to an Organization Virtual Datacenter Network IP Pool

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

**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 Properties.
4. Click the Network Specification tab, type an IP address or a range of IP addresses in the text box, and click Add.
5. Click OK.

Modify an Organization Virtual Datacenter Network Name and Description

As your vCloud Director installation increases, you might want to assign a more descriptive name or description to an existing 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 Properties.
4. Type a new name and optional description and click OK.
Modify an Organization Virtual Datacenter Network DNS Settings

You can change the DNS settings for certain types of organization virtual datacenter networks.

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 Properties.
4. Click the Network Specification tab, type the new DNS information, and click OK.

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, cloud isolated networks, and VLAN IDs. You cannot modify or delete VXLAN network pools.

- Modify a Network Pool Name and Description on page 96
  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 on page 96
  You can add port groups to a network pool that is backed by port groups.

- Add Cloud Isolated Networks to a Network Pool on page 97
  You can add Cloud isolated networks to a VCD network isolation-backed network pool.

- Add VLAN IDs to a Network Pool on page 97
  You can add VLAN IDs to a network pool that is backed by a VLAN.

- Delete a Network Pool on page 97
  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 Cloud Isolated Networks to a Network Pool**

You can add Cloud isolated networks to a VCD network isolation-backed network pool.

**Prerequisites**
A VCD network isolation-backed 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 **Properties**.
3. On the **Network Pool Settings** tab, type the number of VCD isolated networks 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 5-13 lists the basic commands for controlling a cloud cell.

<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,” on page 99.

- **Adding Cloud Cells** on page 98
  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** on page 98
  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** on page 99
  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** on page 99
  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

1. 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.

The following platforms and products are supported.

- VMware vFabric Data Director version 2.7
- Cloud Foundry platform version 1.0

To enable service offering integration, see Using the vCloud API to Enable and Configure vCloud Director Service Offering Integration.

- Register an Extension on page 100
  Register and extension to offer vFabric Data Director or Cloud Foundry services in vCloud Director.

- View or Modify Extension Properties on page 101
  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 on page 101
  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 on page 101
  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 on page 102
  You can unregister an extension to remove access to its services from vCloud Director.
Register an Extension

Register an 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,” on page 99.
- 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,” on page 101.
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,” on page 100.

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 an click Finish.

What to do next
Create service instances for use by virtual machines on the organization virtual datacenter. See “Create a Service Instance,” on page 102.

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,” on page 101.

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,” on page 103.

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,” on page 102.

**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**.
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, ESX/ESXi hosts, datastores, and network switches and ports.

This chapter includes the following topics:

- “Managing vSphere vCenter Servers,” on page 105
- “Managing vSphere ESX/ESXi Hosts,” on page 108
- “Managing vSphere Datastores,” on page 109
- “Managing Stranded Items,” on page 110
- “View Resource Pool Properties,” on page 111
- “View Storage Policy Properties,” on page 111

Managing vSphere 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 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 vShield Settings

If the connection settings for vShield for a vCenter Server change, or if you want to use a different instance of vShield, 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. On the vShield tab, type the new settings and click OK.
Managing vSphere ESX/ESXi Hosts

You can prepare hosts for use with vCloud Director, enable or disable hosts, upgrade, and repair hosts.

Enable or Disable an ESX/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 ESX/ESXi Host to Another

You can move all the virtual machines from one ESX/ESXi host to other hosts in the same cluster. This ability is useful to unprepare a host, or 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 ESX/ESXi Host

When you add an ESX/ESXi host to a vSphere cluster that vCloud Director uses, you must prepare the host before a provider virtual datacenter can use its resources. You can unprepare a host to make it unavailable for use in the vCloud Director environment.

For information about moving virtual machines from one host to another, see “Move Virtual Machines from one ESX/ESXi Host to Another,” on page 108.

You cannot prepare a host that is in lockdown mode. After you prepare a host, you can enable lockdown mode.

Prerequisites

Disable the host and ensure that no virtual machines are running on 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.
3 If you are preparing a host, type a user name and password and click OK. vCloud Director prepares or unprepares the host for all provider virtual datacenters that use its resources.

**Upgrade an ESX/ESXi Host Agent**

vCloud Director installs agent software on each ESX/ESXi host in the installation. If you upgrade your ESX/ESXi hosts, you also need to upgrade your ESX/ESXi host agents.

**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 ESX/ESXi Host**

If the vCloud Director agent on an ESX/ESXi host cannot be contacted, try to repair the host.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Hosts** in the left pane.
2. Right-click the host name and select **Repair Host**.

**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.

**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,” on page 110.

**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,” on page 110.

**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
2. Right-click the resource pool and click Properties.

vCloud Director displays the following 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,” on page 113
- “Delete an Organization,” on page 113
- “Add a Catalog to an Organization,” on page 114
- “Editing Organization Properties,” on page 114
- “Managing Organization Resources,” on page 118
- “Managing Organization vApps and Virtual Machines,” on page 118

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 on page 115
  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 on page 115
  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 on page 115
  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.

  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 on page 117
  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.
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 the System LDAP Settings,” on page 133.

**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></td>
<td><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 the Custom LDAP tab, type the custom LDAP settings for the organization, and click OK.</td>
</tr>
</tbody>
</table>

5 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 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>

5. 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>Organization uses the system notification settings.</td>
</tr>
<tr>
<td>Set organization notification settings</td>
<td>Organization uses its own notification settings. If you select this option, 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>

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,” on page 23.

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 supercede quotas set at the organization level.
6 Select the limits for resource intensive operations.
   Only system administrators can set limits.
7 Select the number of simultaneous connections for each virtual machine and 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,” on page 52.

For information about removing an organization virtual datacenter, see “Delete an Organization Virtual Datacenter,” on page 60.

For information about modifying the resources available to an existing organization virtual datacenter, see “Edit Organization Virtual Datacenter Allocation Model Settings,” on page 61, and “Edit Organization Virtual Datacenter Storage Settings,” on page 61.

**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.
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.

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,” on page 120.

Fast provisioning is enabled by default on organization virtual datacenters. Fast provisioning requires vCenter 5.0 and ESXi 5.0 hosts. If the provider virtual datacenter on which the organization virtual datacenter is based contains ESX/ESXi 4.x hosts, you must disable fast provisioning. See “Edit Organization Virtual Datacenter Storage Settings,” on page 61.

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,” on page 120.

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.
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,” on page 123
- “Import a System Administrator,” on page 124
- “Enable or Disable a System Administrator,” on page 124
- “Delete a System Administrator,” on page 124
- “Edit System Administrator Profile and Contact Information,” on page 125
- “Send an Email Notification to Users,” on page 125
- “Delete a System Administrator Who Lost Access to the System,” on page 125
- “Import a Group,” on page 125
- “Delete an LDAP Group,” on page 126
- “View Group Properties,” on page 126
- “Roles and Rights,” on page 126

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 vCenter Single Sign On,” on page 139.

**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,” on page 123 and “Import a System Administrator,” on page 124.

**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 vCenter Single Sign On,” on page 139.

**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 <strong>Search Groups</strong>.</td>
</tr>
<tr>
<td></td>
<td>b Select the groups to import and click <strong>Add</strong>.</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 <strong>Add</strong>. 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,” on page 125.

**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.

**Roles and Rights**

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

System administrators and organization administrators must assign each user or group a role. The same user can have a different role in different organizations. System administrators can also create roles and modify existing ones.

For information about the predefined roles and their rights, see “Predefined Roles and Their Rights,” on page 147.

- **Create a Role** on page 127

  If the existing roles do not meet your needs, you can create a role and assign rights to the role. When you create a role, it becomes available to all of the organizations in the system.
Copy a Role on page 127
To create a role based on an existing role, you can copy a role and modify its rights.

Edit a Role on page 127
You can modify the name, description, and rights of a role.

Delete a Role on page 127
You can delete a role from the system. You cannot delete the System Administrator role or a role that is in use.

Create a Role
If the existing roles do not meet your needs, you can create a role and assign rights to the role. When you create a role, it becomes available to all of the organizations in the system.

Procedure
1 Click the Administration tab and click Roles in the left pane.
2 Click New.
3 Type a name and optional description for the role.
4 Select the rights for the role and click OK.

Copy a Role
To create a role based on an existing role, you can copy a role and modify its rights.

Procedure
1 Click the Administration tab and click Roles in the left pane.
2 Right-click a role and select Copy to.
3 Type a name and optional description for the role.
4 Select the rights for the role and click OK.

Edit a Role
You can modify the name, description, and rights of a role.

Procedure
1 Click the Administration tab and click Roles in the left pane.
2 Right-click a role and select Properties.
3 Edit the name and optional description for the role.
4 Select the new rights for the role and click OK.

For users who are currently logged in, changes to their role do not take effect until the cache for their current session expires or they log out and log in again.

Delete a Role
You can delete a role from the system. You cannot delete the System Administrator role or a role that is in use.

Prerequisites
Assign a new role to all users with the role you want to delete.
Procedure

1. Click the **Administration** tab and click **Roles** in the left pane.
2. Right-click a role and select **Delete**.
3. Click **Yes** to confirm the deletion.
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,” on page 129
- “General System Settings,” on page 129
- “Editing System Email Settings,” on page 131
- “Configuring Blocking Tasks and Notifications,” on page 132
- “Configuring the System LDAP Settings,” on page 133
- “Customize the vCloud Director Client UI,” on page 136
- “Configuring Public Addresses,” on page 137
- “Configure the Account Lockout Policy,” on page 139
- “Configure vCloud Director to use vCenter Single Sign On,” on page 139

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,” on page 129.

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>
<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 synchronisations.</td>
</tr>
<tr>
<td>Name</td>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</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 ESX/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>
<tr>
<td>Verify vShield Manager certificates</td>
<td>Certificates</td>
<td>Select the check box to allow vCloud Director to communicate only with trusted instances of vShield Manager. Click Browse to locate the JCEKS keystore and type the keystore password.</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>Enable Elastic Allocation Pool</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>
</tbody>
</table>
Editing System Email Settings

You can edit system email settings, including SMTP and notification settings.

- **Configure SMTP Settings** on page 131
  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** on page 131
  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.
4. Type the AMQP port.
   The default port is 5672.
5. Type the exchange.
6. Type the vHost.
7. To use SSL, select the SSL check box and choose one of the certificate options.
   - **Option**: Accept all certificates
     - **Action**: Select the check box.
   - **Option**: SSL Certificate
     - **Action**: Click Browse to locate the SSL certificate.
   - **Option**: SSL Keystore
     - **Action**: Click Browse to locate the SSL keystore. Type the keystore password.
8. 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.
9. Type a user name and password to connect to the AMQP host.
10. Click Test AMQP Connection to test the settings.
11. Click Apply.
12. (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.
5 Click Apply.

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 the System LDAP Settings
You can configure vCloud Director to create user accounts and authenticate user credentials against an LDAP server. Instead of manually creating user accounts, you can import LDAP users and groups by pointing the installation to an LDAP server.

After you connect vCloud Director to an LDAP server, 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 to vCloud Director, vCloud Director checks the credentials of the user against the LDAP directory. If the credentials are accepted, vCloud Director creates a user account and logs the user in to the system.

vCloud Director does not support hierarchical domains for LDAP authentication.

vCloud Director cannot modify the information in your LDAP directory. You can add, delete, or modify LDAP users or groups only in the LDAP directory itself.

You can control how often vCloud Director synchronizes user and group information with the LDAP directory.

LDAP Support
vCloud Director supports various combinations of operating system, LDAP server, and authentication method.

Table 9-2 displays a list of what vCloud Director supports.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>LDAP Server</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003</td>
<td>Active Directory</td>
<td>Simple</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Active Directory</td>
<td>Simple SSL</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Active Directory</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Active Directory</td>
<td>Kerberos SSL</td>
</tr>
<tr>
<td>Windows 2008</td>
<td>Active Directory</td>
<td>Simple</td>
</tr>
<tr>
<td>Windows 7 (2008 R2)</td>
<td>Active Directory</td>
<td>Simple</td>
</tr>
</tbody>
</table>
### Table 9-2. Supported Combinations of Operating System, LDAP Server, and Authentication Method

(Continued)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>LDAP Server</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (2008 R2)</td>
<td>Active Directory</td>
<td>Simple SSL</td>
</tr>
<tr>
<td>Windows 7 (2008 R2)</td>
<td>Active Directory</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows 7 (2008 R2)</td>
<td>Active Directory</td>
<td>Kerberos SSL</td>
</tr>
<tr>
<td>Linux</td>
<td>OpenLDAP</td>
<td>Simple</td>
</tr>
<tr>
<td>Linux</td>
<td>OpenLDAP</td>
<td>Simple SSL</td>
</tr>
</tbody>
</table>

### 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,” on page 135.

#### 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.
   - **Option** | **Action**
   - Accept all certificates | Select the check box.
   - SSL Certificate | Click **Browse** to locate the SSL certificate.
   - SSL Keystore | Click **Browse** to locate the SSL keystore. Type and confirm the keystore password.
6. Select an authentication method.
   - **Option** | **Description**
   - Simple | 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.
   - Kerberos | Kerberos issues authentication tickets to prove a user’s identity. If you select Kerberos, you must select a realm.
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,” on page 129.

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. 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.
2. Select Revert back to system default theme and click Apply.

Configuring Public Addresses
You can configure public Web addresses for the system, including the public Web URL, the public console proxy address, and the public REST API base URL.

Configure the Public Web URL on page 138
If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public web URL.
Configure the Public Console Proxy Address on page 138

If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public console proxy address.

Configure the Public REST API Base URL on page 139

If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public REST API base URL.

Configure the Public Web URL

If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public web URL.

During the initial configuration of each cloud cell, you specified an HTTP service IP address. By default, vCloud Director uses that address to construct the organization URL that organization users access to log in to the system. To use a different address, specify a public web URL.

Procedure

1. Click the Administration tab and click Public Addresses in the left pane.
2. Type the public web URL.
   - If you are using a load balancer, set the public web URL to the load balancer’s IP (ex. https://LoadBalancerIP). If you are not using a load balancer, you must include /cloud at the end of your public web URL (ex. https://cellIP/cloud).
3. Click Apply.

When you create an organization, its organization URL includes the public web URL instead of the HTTP service IP address. vCloud Director also modifies the organization URLs of existing organizations.

Configure the Public Console Proxy Address

If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public console proxy address.

During the initial configuration of each cloud cell, you specified a remote console proxy IP address. By default, vCloud Director uses that address when a user attempts to view a virtual machine console. To use a different address, specify a public console proxy address.

Procedure

1. Click the Administration tab and click Public Addresses in the left pane.
2. Type the hostname or IP address for the public console proxy address.
   - This can be the address of the load balancer or some other machine that can route traffic to the remote console proxy IP.
3. Click Apply.

Remote console session tickets sent to the HTTP service IP address return the public console proxy address.
Configure the Public REST API Base URL

If your vCloud Director installation includes multiple cloud cells running behind a load balancer or NAT, or if the cloud cells do not have publicly-routable IP addresses, you can set a public REST API base URL.

During the initial configuration of each cloud cell, you specified an HTTP service IP address. By default, vCloud Director uses that address in the XML responses from the REST API and as the upload target for the transfer service (for uploading vApp templates and media). To use a different address, specify a public REST API base URL.

Procedure

1. Click the Administration tab and click Public Addresses in the left pane.
2. Type the hostname or IP address for the public REST API base URL.
   - This can be the address of the load balancer or some other machine that can route traffic to the HTTP service IP.
3. Click Apply.

XML responses from the REST API include the base URL and the transfer service uses the base URL as the upload target.

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 Password Policy 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 vCenter Single Sign On

When vCenter Single Sign On is configured and enabled, system administrators are authenticated by the vSphere identity provider.

Prerequisites

Set up vCenter Single Sign On and take note of the vCenter Lookup URL. See the vSphere documentation.

Procedure

1. Click the Administration tab and click Federation in the left pane.
2. Click Register.
3. Type the vCenter Lookup Service URL.
4. Type the user name of the vSphere Single Sign On user with administrator privileges.
5 Type the vSphere Single Sign On password for the user name entered above.
6 Click OK.
7 Select Use vSphere Single Sign-On and click Apply.

System administrators are asked for vCenter Single Sign On credentials to log in to vCloud Director.

**What to do next**

Import vCenter Single Sign On users and groups. See “Import a System Administrator,” on page 124 and “Import a Group,” on page 125.
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,” on page 141
- “Monitor and Manage Blocking Tasks,” on page 143
- “View Usage Information for a Provider Virtual Datacenter,” on page 143
- “View Usage Information for an Organization Virtual Datacenter,” on page 143
- “Using vCloud Director’s JMX Service,” on page 144
- “Viewing the vCloud Director Logs,” on page 144
- “vCloud Director and Cost Reporting,” on page 145

Viewing Tasks and Events

You can view system tasks and events and organization tasks and events to monitor and audit vCloud Director 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,” on page 142.

The log can also include debug information, depending on your vCloud Director settings. See “General System Settings,” on page 129.
**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,”** on page 141.

The log can also include debug information, depending on your vCloud Director settings. See “**General System Settings,”** on page 129.

**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,”** on page 142.

**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,”** on page 142.
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.

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 <strong>Error</strong>.</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>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. This log also shows warnings or</td>
</tr>
<tr>
<td></td>
<td>errors encountered by the cell.</td>
</tr>
<tr>
<td>vmware-vcd-watchdog.log</td>
<td>Informational log messages from the cell watchdog. It records when the</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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 1.5 to configure a cost reporting system for VMware vCloud Director.

See the *VMware vCenter Chargeback User’s Guide* for more information.

You can specify the number of days of chargeback history that vCloud Director saves. See “Modify General System Settings,” on page 129.
vCloud Director uses roles, and their associated rights, to determine which users and groups can perform which operations. System administrators can create and modify roles. System administrators and organization administrators can assign roles to users and groups in an organization.

vCloud Director includes several predefined roles.

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

**Predefined Roles and Their Rights**

vCloud Director includes predefined roles. Each of these roles includes a set of default rights.

**System Administrator**

The system administrator has super-user rights to all objects in the system. 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 this role.

**Organization Roles**

After creating an organization, a system administrator can assign the role of organization administrator to any user in the organization. An organization administrator has super-user rights within that organization, and can assign any of the predefined roles to the organization’s users and groups.

- **Organization Administrator**
  An organization administrator can assign the role of organization administrator to any member of an organization.

- **Catalog Author**
  The rights associated with the catalog author role allow a user to create and publish catalogs.

- **vApp Author**
  The rights associated with the vApp Author role allow a user to use catalogs and create vApps.
**vApp User**

The rights associated with the vApp User role allow a user to use existing vApps.

**Console Access Only**

The rights associated with the 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 will be 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. If an organization administrator modifies the set of rights associated with a predefined role, those modifications apply only in the context of that organization. If a system administrator modifies the set of rights associated with a predefined role, those modifications apply to all organizations in the system.

You classify rights according to the objects to which they apply.

### Rights Associated with Catalogs

**Table 11-1. Rights Associated With Catalogs**

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog: Add vApp from My Cloud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Change Owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Create/Delete a Catalog</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Edit Catalog Properties</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Allow External Publishing/Subscriptions for the Catalogs</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Rights Associated With Catalogs (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog: Share a Catalog to Users/Groups within Current Organization</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to share catalogs to users and groups in the same organization.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View Private and Shared Catalogs within Current Organization</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to view both private and shared catalogs in the organization.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View Shared Catalogs from Other Organizations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to view catalogs shared from other organizations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rights Associated with Independent Disks

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk: Create</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to create independent disks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: Delete</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to delete independent disks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: Edit Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to edit the properties of an independent disk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk: View Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Permission to view the properties of an independent disk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rights Associated with vApp Templates and Media

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog Item: Add to My Cloud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Permission to add a vApp template or media file to My Cloud.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Copy/Move a vApp Template/Media</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission to copy and move vApp templates and media files.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 11-3. Rights Associated With vApp Templates and Media (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog Item: Create/Upload a vApp Template/Media</td>
<td>Permission to create and upload vApp templates and media files.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Enable vApp Template/Media Download</td>
<td>Permission to enable a vApp template or media item to be downloaded.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Edit vApp Template/Media Properties</td>
<td>Permission to edit the properties of a vApp template or media file.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: View vApp Templates/Media</td>
<td>Permission to view vApp templates and media files.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Rights Associated with vApps

Table 11-4. Rights Associated With vApps

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<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>
</tr>
<tr>
<td>vApp: Copy a vApp</td>
<td>Permission to copy a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Create/Reconfigure a vApp</td>
<td>Permission to create and reconfigure vApps.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Delete a vApp</td>
<td>Permission to delete a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Download a vApp</td>
<td>Permission to download a vApp.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit vApp Properties</td>
<td>Permission to edit a vApp’s properties.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit VM CPU</td>
<td>Permission to edit virtual machine CPUs.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Hard Disk</td>
<td>Permission to edit virtual machine hard disks.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Memory</td>
<td>Permission to edit virtual machine memory.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Network</td>
<td>Permission to edit virtual machine network configuration.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Table 11-4. Rights Associated With vApps (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp: Edit VM Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Manage VM Password Settings</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Start/Stop/Suspend/Reset a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Share a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Create/Remove/Revert a Snapshot</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Upload a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Access to a VM Console</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: View VM Metrics</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Insert CD</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Administrative Rights

All of these rights are granted to the system administrator throughout the system, and to an organization administrator within the organization. These rights are not granted to any other predefined role.

### Table 11-5. Other Administrative Rights

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>General: Administrator Control</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General: Administrator View</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General: Send Notification</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway: Configure Services</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Admin</td>
<td>Catalog Author</td>
<td>vApp Author</td>
<td>vApp User</td>
<td>Console Access Only</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Organization VDC Network: Edit Properties</td>
<td>Permission to edit the properties of an organization virtual data center network.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization VDC Network: View Properties</td>
<td>Permission to view the properties of an organization virtual data center network.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization VDC: Set Default Storage Policy</td>
<td>Permission to set the default storage policy for an organization virtual data center.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization VDC: View Organization VDCs</td>
<td>Permission to view organization virtual data centers.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Federation Settings</td>
<td>Permission to edit an organization’s federation settings.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Leases Policy</td>
<td>Permission to edit an organization’s leases policy.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Organization Network Properties</td>
<td>Permission to edit an organization’s network properties</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Organization Properties</td>
<td>Permission to edit organization properties.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Password Policy</td>
<td>Permission to edit an organization’s password policy.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Quotas Policy</td>
<td>Permission to edit an organization’s quotas policy.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit SMTP Settings</td>
<td>Permission to edit an organization’s SMTP settings.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit Organization Associations</td>
<td>Permission to edit an organization’s associations.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: View Organization Networks</td>
<td>Permission to view organization networks.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 11-5. Other Administrative Rights (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization: View</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Organizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization: Edit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X (system administrator only)</td>
</tr>
<tr>
<td>Operation Limits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Index

A
account lockout 139
activity log 141, 142
adding resources 15
adding vSphere resources 15
allocation pool 24
allocation models 31, 32, 54, 55
allocation pool allocation model 31, 54
AMQP broker 132

B
blocking tasks
about 132
configuring settings 132
configuring tasks 133
branding the UI
revert to system logo 137
revert to system theme 137

C
catalog publishing, enabling 37
catalogs
adding 114
creating 38
external publishing 42
publishing 37
sharing 41
subscribe 42
certificates, replacing 13
changing your password 14
Cisco Nexus 1000V 20
Cloud Foundry 99, 100
cloud cells
adding 98
deleting 98
maintenance message 99
managing 98
restarting 98
starting 98
stopping 98
cloud resources 17, 45
cost reporting 145
datasstores
disk space warnings 51, 109
enabling and disabling 109
monitoring capacity 51
DHCP network services 68, 86

E
edge gateway
add 34, 57, 67
adding 65
adding a firewall rule 70
apply syslog server settings 82
configuring DHCP 68
configuring firewalls 69
create VPN tunnel 72, 74
deleting 81
description 67
DNS 35, 58, 66, 80
enabling site-to-site VPN 71
enabling static routing 75
external networks 35, 58, 66, 80
gateway configuration 34, 57, 66
HA 79
high availability 79
IP address 35, 58, 66, 80
IP pools 35, 58, 66, 80
load balancing 75
name 67
ordering firewall rules 71
organization virtual datacenter 66
properties 79
rate limits 35, 58, 67, 81
services 68
upgrading 81
viewing IP usage 82
elastic virtual datacenter 31, 49, 54
e-mail notifications 52, 125, 131
e-mail settings 131
ESXi/ESXi hosts
enabling and disabling 46, 108
moving virtual machines 108
preparing and unpreparing 47, 108
repairing 47, 109
upgrading agent 47, 109
extension 100
extensions
aborting 143
add service offering 101
add services 101
configuring AMQP 132
delete 102
failing 143
remove 102
resuming 143
external networks
adding 19
adding IP addresses 64
defined 18
deleting 64
name and description 63
specification 63, 64

F
fast provisioning 33, 56, 61, 110, 120
firewall rules, setting the order 71, 88

G
general system settings 129
getting started 9
groups, view 126
guided tasks 12

H
Home tab 12

I
identity provider 139
importing
media files 41
vApp templates 40

J
JMX, accessing 144
JMX service 144

K
Kerberos realm 135

L
LDAP
configuring 133
customizing attributes 136
setting up the connection 134
support 133
synchronizing 136
testing the connection 135
leases, runtime and storage 23
licensing, vShield 17
linked clones 120
load balancer 138, 139
load balancing
pool servers 76, 77
server pools 78
virtual servers 78, 79
logging in 12
logs 144
Lost & Found 125

M
MBeans 144
media, uploading 40
monitoring, tasks and events 141
monitoring vCloud Director 141
MTU 22

N
NAT 68, 69
Network Address Translation 68, 69
network pools
adding Cloud isolated networks 97
adding port groups 96
adding VLAN IDs 97
cloud network isolation-backed 21
defined 19
deleting 97
name and description 96
port group-backed 20
setting the MTU 22
VLAN-backed 20
VXLAN 19
network quota 34, 57
network services 85
Nexus 1000V 20
notifications, about 132

O
organization virtual datacenter networks
adding a firewall rule 87
adding a static route 90, 92
adding IP addresses 95
configuring DHCP 86
configuring firewalls 86
configuring services 85
connected vApp templates 94
connected vApps 94
create VPN tunnel 73, 89
creating 36, 59, 83
deleting 94
enabling site-to-site VPN 88
enabling static routing 90
external direct 84
external NAT-routed 84
internal 85
managing 82
modifying DNS 96
modifying the name and description 95
ordering firewall rules 88
properties 95
resetting 93
viewing IP usage 94
organization virtual datacenters
  allocating storage 33, 56
  allocation models 32, 55
  allocation model settings 61
  changing description 60
  changing name 60
  confirm settings 36, 59
  creating 31, 52, 53
  deleting 60
  enabling or disabling 60
  monitoring usage 143
  naming 36, 59
  network pools 62
  network quota 34, 57
  properties 60
  selecting a network pool 34, 57
  selecting a provider virtual datacenter 31, 54
  selecting the organization 54
  storage capacity 61
organizations
  adding local users 27
  allocating resources 30, 31
  confirm settings 29
  creating 25, 26
  deleting 113
  email preferences 28, 117
  enabling or disabling 113
  full name and description 115
  LDAP options 27, 115
  lease settings 29, 117
  limit settings 29, 117
  managing 113
  managing resources 118
  monitoring events 142
  monitoring tasks 142
  naming 26
  properties 114
  publishing catalogs 28, 116
  quota settings 29, 117
  renaming 115
  SMTP server 28
  SMTP settings 117
  vApps 118
  OVF upload 39

P
password policy 139
pay-as-you-go 24
pay-as-you-go allocation model 31, 54
peer settings 74
pool servers
  add 76
  edit 77
  settings 77
provider virtual datacenter
  allocation pool 24
  pay-as-you-go 24
  reservation pool 24
provider virtual datacenters
  adding resource pools 49
  changing name 46
  creating 17
  datastores 48
  defined 17
  deleting 46
  enabling or disabling 45
  managing 45
  monitoring usage 143
Provider virtual datacenters, merging 46
public addresses 137
public IP address 72
publishing catalogs 37
publishing catalogs externally 42
Q
quick start tasks 12
R
reservation pool 24
reservation pool allocation model 31, 54
resource pools
  CPU reservation 111
datastores 111
detach 50
disable 50
enable 50
memory reservation 111
roles
  copying 127
  creating 127
  deleting 127
  editing 127
  roles and rights 147
runtime leases 23
S
server pools, delete 78
service instance
    add to a virtual machine 103
description 102
name 102
parameters 102
service offering 99, 100
service offerings
    add 101
    create 101
    create instance 102
delete instance 103
disassociate 101
remove 101
services
    create instance 102
delete instance 103
shadow virtual machines 120
sharing catalogs 41
single sign-on 139
SMTP server 117
SMTP settings 131
SSO 139
storage policies
    add 49, 62
datastores 111
name 49
type 49
value 49
storage leases 23
stranded items
    deleting 110
    force deleting 110
system
    monitoring tasks 141
    roles and rights 126
system administrators
    creating accounts 123
deleting 124
    disabling 124
    editing accounts 125
from LDAP 124
LDAP groups 125, 126
vCenter Single Sign On groups 125
vSphere SSO groups 125
system events 142
system notification settings 131
system settings, email 131

T
Technical Support, to obtain 7
thin provisioning 33, 56, 61

U
upgrade vCenter Server 107
uploading
    media 40
    vApps 39
user preferences 14

V
VAAI 110
vApps
    adding vSphere virtual machines 118
    backing up 119
    force stopping 120
    importing from vSphere 119
    placing in maintenance mode 119
vCenter Server, upgrade 107
vCenter Chargeback 145
vCenter Servers
    assigning a vShield license 17
    attaching 15, 16
    confirming settings 16
    connecting 16
    connection settings 105, 106
    disabling 106
    reconnecting 106
    removing 107
vShield settings 107
vCloud Director overview 9
vFabric 99
vFabric Data Director 100
virtual machines
    add service instance 103
    importing from vSphere 118, 119
    migrate 51
virtual servers
    add 78
delete 79
edit 78
    settings 78
VPN
    edit 75
    settings 75
VPN tunnel
    peer settings 74
remote 74
vShield
    connecting 16
    licensing 17
    settings 107
vShield for VMware Cloud Director license 17
vSphere

datastores 109
importing media files from 41
importing virtual machines from 40
resources 105
stranded items 110
vSphere distributed switches, setting the
MTU 22
vSphere lookup service 139
vSphere VXLAN 48
VXLAN 19, 48

W
web addresses 137
Web console, logging in 12