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
Contents

vCloud Director Administrator’s Guide  7

Updated Information  9

1 Getting Started with vCloud Director  11
   Overview of vCloud Director Administration  11
   Log In to the Web Console  13
   Preparing the System  14
   Create a Microsoft Sysprep Deployment Package  14
   Replace a Microsoft Sysprep Deployment Package  15
   Replace SSL Certificates  16
   Set User Preferences  17

2 Adding Resources to vCloud Director  19
   Adding vSphere Resources  19
   Adding Cloud Resources  21

3 Creating and Provisioning Organizations  27
   Understanding Leases  27
   Create an Organization  28
   Allocate Resources to an Organization  32

4 Creating a Published Catalog  41
   Enable Catalog Publishing  41
   Create a Published Catalog  42
   Upload a vApp Template  42
   Import a vApp Template from vSphere  43
   Upload a Media File  43
   Import a Media File from vSphere  44
   Publish a Catalog  44

5 Managing Cloud Resources  45
   Managing Provider vDCs  45
   Managing Organization vDCs  52
   Managing External Networks  64
   Managing Edge Gateways  65
   Managing Organization vDC Networks  81
   Managing Network Pools  94
   Managing Cloud Cells  96
6 Managing vSphere Resources  99
   Managing vSphere vCenter Servers  99
   Managing vSphere ESX/ESXi Hosts  101
   Managing vSphere Datastores  102
   Managing Stranded Items  103

7 Managing Organizations  105
   Enable or Disable an Organization  105
   Delete an Organization  105
   Add a Catalog to an Organization  106
   Editing Organization Properties  106
   Managing Organization Resources  110
   Managing Organization Users and Groups  110
   Managing Organization vApps and Virtual Machines  110

8 Managing System Administrators and Roles  113
   Add a System Administrator  113
   Import a System Administrator  113
   Enable or Disable a System Administrator  114
   Delete a System Administrator  114
   Edit System Administrator Profile and Contact Information  114
   Send an Email Notification to Users  115
   Delete a System Administrator Who Lost Access to the System  115
   Import a Group  115
   Delete an LDAP Group  116
   View Group Properties  116
   Roles and Rights  116

9 Managing System Settings  119
   Modify General System Settings  119
   General System Settings  119
   Editing System Email Settings  121
   Configuring Blocking Tasks and Notifications  122
   Configuring the System LDAP Settings  123
   Customize the vCloud Director Client UI  126
   Configuring Public Addresses  127
   Configure the Account Lockout Policy  129
   Configure vCloud Director to use vCenter Single Sign On  129

10 Monitoring vCloud Director  131
   Viewing Tasks and Events  131
   Monitor and Manage Blocking Tasks  133
   View Usage Information for a Provider vDC  133
   View Usage Information for an Organization vDC  133
   Using vCloud Director's JMX Service  134
   Viewing the vCloud Director Logs  134
   vCloud Director and Cost Reporting  134
   Monitoring Quarantined Files  135
11 Roles and Rights 137
   Predefined Roles and Their Rights 137

Index 141
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.
This *vCloud Director Administrator’s Guide* is updated with each release of the product or when necessary.

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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000817-01</td>
<td>Added Edge Gateway creation and configuration to the organization vDC creation and organization resource allocation workflows.</td>
</tr>
<tr>
<td></td>
<td>Removed an obsolete procedure from the managing provider vDCs section.</td>
</tr>
<tr>
<td>000817-00</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Getting Started with vCloud Director

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

You can also set your user preferences and create a Microsoft Sysprep deployment package to support guest customization in vCloud Director virtual machines.

This chapter includes the following topics:

- “Overview of vCloud Director Administration,” on page 11
- “Log In to the Web Console,” on page 13
- “Preparing the System,” on page 14
- “Create a Microsoft Sysprep Deployment Package,” on page 14
- “Replace a Microsoft Sysprep Deployment Package,” on page 15
- “Replace SSL Certificates,” on page 16
- “Set User Preferences,” on page 17

**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 vDC 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 (vDC) 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 vDCs for users in different geographic locations or business units, or for users with different performance requirements.

Organization Virtual Datacenters

An organization virtual datacenter (vDC) provides resources to an organization and is partitioned from a provider vDC. Organization vDCs 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 vDCs.

vCloud Director Networking

vCloud Director supports three types of networks.

- External networks
- organization vDC networks
- vApp networks

Some organization vDC 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 vDC 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 vDC Networks

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

Only system administrators can create organization vDC networks. System administrators and organization administrators can manage organization vDC 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 vDC network to allow the vApp to communicate with other vApps in the organization and outside of the organization, if the organization vDC 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 vDC. 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 vDC networks and all vApp networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Each organization vDC in vCloud Director can have one network pool. Multiple organization vDCs can share the same network pool. The network pool for an organization vDC provides the networks created to satisfy the network quota for an organization vDC.

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.
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 19</td>
</tr>
<tr>
<td>Create a Provider Virtual Datacenter</td>
<td>“Create a Provider Virtual Datacenter,” on page 21</td>
</tr>
<tr>
<td>Create an External Network</td>
<td>“Add an External Network,” on page 22</td>
</tr>
<tr>
<td>Create a Network Pool</td>
<td>“Network Pools,” on page 23</td>
</tr>
<tr>
<td>Create an Organization</td>
<td>“Create an Organization,” on page 28</td>
</tr>
<tr>
<td>Allocate Resources to an Organization</td>
<td>“Create an Organization vDC,” on page 52</td>
</tr>
<tr>
<td>Add a Network to an Organization</td>
<td>“Adding Networks to an Organization vDC,” on page 81</td>
</tr>
<tr>
<td>Add a Catalog to an Organization</td>
<td>“Add a Catalog to an Organization,” on page 106</td>
</tr>
</tbody>
</table>

Create a Microsoft Sysprep Deployment Package

Before vCloud Director can perform guest customization on virtual machines with certain Windows guest operating systems, you must create a Microsoft Sysprep deployment package on each cloud cell in your installation.

During installation, vCloud Director places some files in the sysprep folder on the vCloud Director server host. Do not overwrite these files when you create the Sysprep package.

Prerequisites


Procedure

1. Copy the Sysprep binary files for each operating system to a convenient location on a vCloud Director server host.

   Each operating system requires its own folder.

   NOTE: Folder names are case-sensitive.

<table>
<thead>
<tr>
<th>Guest OS</th>
<th>Copy Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 (32-bit)</td>
<td>SysprepBinariesDirectory /win2k3</td>
</tr>
<tr>
<td>Windows 2003 (64-bit)</td>
<td>SysprepBinariesDirectory /win2k3_64</td>
</tr>
<tr>
<td>Windows XP (32-bit)</td>
<td>SysprepBinariesDirectory /winxp</td>
</tr>
<tr>
<td>Windows XP (64-bit)</td>
<td>SysprepBinariesDirectory /winxp_64</td>
</tr>
</tbody>
</table>

SysprepBinariesDirectory represents a location you choose to which to copy the binaries.
2 Run the `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh SysprepBinariesDirectory` command.

   For example, `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

3 Use the service `vmware-vcd restart` command to restart the cloud cell.

4 If you have multiple cloud cells, copy the package and properties file to all cloud cells.

   `scp /opt/vmware/vcloud-director/guestcustomization/vcloud_sysprep.properties /opt/vmware/vcloud-director/guestcustomization/windows_deployment_package_sysprep.cab root@next_cell_IP:/opt/vmware/vcloud-director/guestcustomization`

5 Restart each cloud cell to which you copy the files.

### Replace a Microsoft Sysprep Deployment Package

If you already created a Microsoft Sysprep deployment package and you need to generate a new one, you must replace the existing Sysprep package on each cloud cell in your installation.

#### Prerequisites


#### Procedure

1 Use the service `vmware-vcd stop` command to stop the first cloud cell.

2 Copy the new Sysprep binary files for each operating system to a convenient location on a vCloud Director server host.

   Each operating system requires its own folder.

   **NOTE** Folder names are case-sensitive.

<table>
<thead>
<tr>
<th>Guest OS</th>
<th>Copy Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 (32-bit)</td>
<td><code>SysprepBinariesDirectory /win2k3</code></td>
</tr>
<tr>
<td>Windows 2003 (64-bit)</td>
<td><code>SysprepBinariesDirectory /win2k3_64</code></td>
</tr>
<tr>
<td>Windows XP (32-bit)</td>
<td><code>SysprepBinariesDirectory /winxp</code></td>
</tr>
<tr>
<td>Windows XP (64-bit)</td>
<td><code>SysprepBinariesDirectory /winxp_64</code></td>
</tr>
</tbody>
</table>

   `SysprepBinariesDirectory` represents a location you choose to which to copy the binaries.

3 Run the `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh SysprepBinariesDirectory` command.

   For example, `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

4 Use the service `vmware-vcd restart` command to restart the cloud cell.

5 If you have multiple cloud cells, stop each cell and copy the package and properties file to each cell.

   `scp /opt/vmware/vcloud-director/guestcustomization/vcloud_sysprep.properties /opt/vmware/vcloud-director/guestcustomization/windows_deployment_package_sysprep.cab root@next_cell_IP:/opt/vmware/cloud-director/guestcustomization`

6 Restart each cloud cell to which you copy the files.
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:
   ```bash
   /opt/vmware/vcloud-director/bin/configure
   ```
4. Specify the full path to the Java keystore file that holds the new certificates.
   ```text
   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.
   ```text
   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.
Adding Resources to vCloud Director

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

This chapter includes the following topics:
- “Adding vSphere Resources,” on page 19
- “Adding Cloud Resources,” on page 21

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 Manager 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 20
   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 20
   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 Manager on page 20
   vCloud Director requires vShield Manager to provide network services. Each vCenter Server you attach to vCloud Director requires its own vShield Manager.

4. Confirm Settings and Attach the vCenter Server on page 20
   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 Manager

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

Procedure
1. Type the host name or IP address of the vShield Manager to use with the vCenter Server that you are attaching.
2. Type the user name and password to connect to vShield Manager.
   - The default user name is **admin** and the default password is **default**. You can change these defaults in the vShield Manager 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 Manager.
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 vDC 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 32.

For more information about organization vDC networks, see “Managing Organization vDC Networks,” on page 81

**Provider Virtual Datacenters**

A provider virtual datacenter (vDC) 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 vDC is the source for organization vDCs.

**Create a Provider Virtual Datacenter**

You can create a provider vDC to register vSphere compute, memory, and storage resources for vCloud Director to use. You can create multiple provider vDCs for users in different geographic locations or business units, or for users with different performance requirements.

A provider vDC can only include 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 that is configured to use automated DRS. The vCenter Server must have the vShield for VMware vCloud Director license key.

**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 vDC, 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 vDCs based on this provider vDC. **Hardware Version 9** requires ESXi 5.1 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 profiles for the provider vDC to support, click Add, and click Next.
7. Click Finish to create the provider vDC.

**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 vDC networks. For more information about organization vDC networks, see “Managing Organization vDC Networks,” on page 81.

**Add an External Network**

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

**Prerequisites**

A vSphere port group is available. 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 vDC network that connects to the external network.

**Network Pools**

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

A network pool is backed by vSphere network resources such as VLAN IDs, port groups, or Cloud isolated networks. vCloud Director uses network pools to create NAT-routed and internal organization vDC networks and all vApp networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Each organization vDC in vCloud Director can have one network pool. Multiple organization vDCs can share the same network pool. The network pool for an organization vDC provides the networks created to satisfy the network quota for an organization vDC.

**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 vDC networks.

**Prerequisites**

Verify that a range of VLAN IDs and a vSphere distributed switch are available in vSphere. The VLAN IDs must be valid IDs that are configured in the physical switch to which the 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 vDC network that is backed by the network pool or associate the network pool with an organization vDC 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 vDC network that is backed by the network pool or associate the network pool with an organization vDC 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 25.

Add a Network Pool That Is Backed by vSphere Port Groups
You can add a network pool that is backed by port groups to register vSphere port groups for vCloud Director to use. Unlike other types of network pools, a network pool that is backed by port groups does not require a vSphere distributed switch.

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

VXLAN Network Pools

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

When you create a provider vDC, a VXLAN network pool is created in vCloud Director. When you use this network pool, VXLAN virtual wires are created in vCenter Server.

This pool is given a name derived from the name of the containing provider vDC and attached to it at creation. You cannot delete or modify this network pool. You cannot create a VXLAN network pool by any other method. If you rename a provider vDC, 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 on VXLAN in a vCloud environment, see the vShield Administration Guide.
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 27
- “Create an Organization,” on page 28
- “Allocate Resources to an Organization,” on page 32

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 31.

Users can configure email notification to receive a message before a runtime or storage lease expires. See “Set User Preferences,” on page 17 for information about lease expiration preferences.
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 28
   Open the New Organization wizard to start the process of creating an organization.

2. **Name the Organization** on page 29
   Provide a descriptive name and an optional description for your new organization.

3. **Specify the Organization LDAP Options** on page 29
   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 30
   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 Publishing Policy** on page 30
   A catalog provides organization users with a library of vApp templates and media that they can use to create vApps and install applications on virtual machines.

6. **Configure Email Preferences** on page 30
   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 31
   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 31
   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 123.

**Procedure**

1. Select the source for organization users.

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

2. Provide any additional information that your selection requires.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Click <strong>Next</strong>.</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 <strong>Next</strong>. If you do not enter anything, you can import all users in the system LDAP service into the organization. <strong>Note</strong>: Specifying an OU does not limit the LDAP groups you can import. You can import any LDAP group from the system LDAP root. However, only users who are in both the OU and the imported group can log in to the organization.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Click <strong>Next</strong> and enter the custom LDAP settings for the organization.</td>
</tr>
</tbody>
</table>
Add Local Users to the Organization

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

Procedure
1. Click Add.
2. Type a user name and password.
3. Assign a role to the user.
4. (Optional) Type the contact information for the user.
5. Select Unlimited or type a user quota for stored and running virtual machines and click OK.
   These quotas limit the user’s ability to consume storage and compute resources in the organization.
6. Click Next.

Set the Organization Catalog Publishing Policy

A catalog provides organization users with a library of vApp templates and media that they can use to create vApps and install applications on virtual machines.

Generally, catalogs should only be available to users in a single organization, but a system administrator can allow the organization administrator to publish their catalogs to all organizations in the vCloud Director installation.

Procedure
1. Select a catalog publishing option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot publish catalogs</td>
<td>The organization administrator cannot publish catalogs for users outside of the organization.</td>
</tr>
<tr>
<td>Allow publishing catalogs to all organizations</td>
<td>The organization administrator can publish catalogs for users in all organizations.</td>
</tr>
</tbody>
</table>

2. Click Next.

Configure Email Preferences

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

Procedure
1. Select an SMTP server option.

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


2 Select a notification settings option.

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

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

4 Click Next.

### Configure Organization Lease, Quota, and Limit Settings

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

For more information about leases, see “Understanding Leases,” on page 27.

**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.

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 vDC that is partitioned from a provider vDC. A single organization can have multiple organization vDCs.

**Prerequisites**

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

**Procedure**

1. **Open the Allocate Resources Wizard** on page 33
   
   Open the Allocate Resources wizard to start the process of creating an organization vDC for an organization.

2. **Select a Provider vDC** on page 33
   
   An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC provides these resources to vApps and virtual machines in the organization.

3. **Select an Allocation Model** on page 34
   
   The allocation model determines how and when the provider vDC compute and memory resources that you allocate are committed to the organization vDC.

4. **Configure the Allocation Model** on page 36
   
   Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.

5. **Allocate Storage** on page 37
   
   An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC datastores.

6. **Select Network Pool and Services** on page 38
   
   A network pool is a group of undifferentiated networks used to create vApp networks and internal organization vDC networks.

7. **Configure an Edge Gateway** on page 38
   
   You configure an edge gateway to provide connectivity to one or more external networks.

8. **Configure External Networks** on page 39
   
   Select the external networks that the edge gateway can connect to.

9. **Configure IP Settings on a New Edge Gateway** on page 39
    
    Configure IP settings for external networks on the new edge gateway.

10. **Suballocate IP Pools on a New Edge Gateway** on page 39
    
    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 39
    
    Configure the inbound and outbound rate limits for each external network on the edge gateway.

12. **Create an Organization vDC Network** on page 40
    
    You can create an organization vDC network that is connected to the new edge gateway.
13 Name the Organization vDC on page 40
   You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization vDC.

14 Confirm Settings and Create the Organization vDC on page 40
   Before you create the organization vDC, 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 vDC 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 vDC
An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC provides these resources to vApps and virtual machines in the organization.

Procedure
1 Select a provider vDC.
   The provider vDC list displays information about available resources and the networks list displays information about networks available to the selected provider vDC.
2 Click Next.
Select an Allocation Model

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

Procedure

1. Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>Only a percentage of the resources you allocate from the provider vDC are committed to the organization vDC. You can specify the percentage for both CPU and memory. This percentage is known as the percentage guarantee factor, and it allows you to overcommit resources. Starting with vCloud Director 5.1, Allocation Pool organization vDCs are elastic by default. This means that the organization vDC spans and utilizes all resource pools associated with its provider vDC. As a result, vCPU frequency is now a mandatory parameter for an Allocation Pool. Set the vCPU frequency and percentage guarantee factor in such a way that a sufficient number of virtual machines can be deployed on the organization vDC without CPU being a bottleneck factor. When a virtual machine is created, the placement engine places it on a provider vDC resource pool that best fits the requirements of the virtual machine. A sub-resource pool is created for this organization vDC under the provider vDC resource pool, and the virtual machine is placed under that sub-resource pool. When the virtual machine powers on, the placement engine checks the provider vDC resource pool to ensure it still has the capacity to power on the virtual machine. If not, the placement engine moves the virtual machine to a provider vDC resource pool with sufficient resources to run the virtual machine. A sub-resource pool for the organization vDC is created if one does not already exist. The sub-resource pool is configured with sufficient resources to run the new virtual machine. The sub-resource 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 vDC. The sub-resource pool’s CPU limit is increased by the number of vCPU the virtual machine is configured with times the vCPU frequency specified at the organization vDC level, and the CPU reservation is increased by the number of vCPU configured for the virtual machine times the vCPU specified at the organization vDC level times the percentage guarantee factor for CPU set at the organization vDC level. The virtual machine is reconfigured to set its memory and CPU reservation to zero and placed. 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 sub-resource pool and that this model can take advantage of new resources added to the provider vDC. In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power on because of a lack of resources on the original resource pool. This might involve a minor cost to move the virtual machine disk files to a new resource pool.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are only committed when users create vApps in the organization vDC. You can specify a percentage of resources to guarantee, which allows you to overcommit resources. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC. Resources committed to the organization are applied at the virtual machine level.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>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 there is no sub-resource pool 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. The benefit of the Pay-As-You-Go model is that it can take advantage of new resources added to the provider vDC. In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power on due to a lack of resources on the original resource pool. This 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 are also unable to take advantage of the resources of idle virtual machines on the same sub-resource pool, since resources are set at the virtual machine level.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization vDC. Users in the organization can control overcommitment by specifying reservation, limit, and priority settings for individual virtual machines. Because there is only one resource pool and one sub-resource pool 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 very fine control over virtual machine rate, limit, and shares, which can lead to optimal usage of the reserved resources if you plan carefully. In this model, reservation is always done at the primary cluster. If there are not sufficient resources to create an organization vDC on the primary cluster, the organization vDC creation fails. Other limitations of this model are that it is not elastic and organization users might set non-optimal shares, rates, and limits on virtual machines, leading to underutilization of resources.</td>
</tr>
</tbody>
</table>

For information on 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 vDC resources to allocate to the organization vDC.

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

2. Click Next.

Example: Configuring an Allocation Model

When you create an organization vDC, 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

<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 Sub-Resource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>The 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>The sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>2.5GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>The 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>The 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 3-2. 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 vDCs always have no reservations or limits. Pay-As-You-Go settings only affect overcommitment. A 100 percent guarantee means no overcommitment is possible. The lower the percentage, the more overcommitment is possible.

Table 3-3. 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>25 GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Allocate Storage

An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC 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 112.

**IMPORTANT** Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider vDC on which the organization vDC is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider vDC on which the organization vDC 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 profile 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 profile used for all virtual machine provisioning operations where the storage profile is not specified.
4. (Optional) Select the **Enable thin provisioning** check box to enable thin provisioning for virtual machines in the organization vDC.
5. (Optional) Deselect the **Enable fast provisioning** check box to disable fast provisioning for virtual machines in the organization vDC.
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 vDC 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. Select Manual from the drop-down menu for each external network for which to specify an IP address.
2. 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 vDC Network

You can create an organization vDC 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 vDC network.
3. (Optional) Select Share this network with other vDCs in the organization.
4. Type a gateway address and network mask for the organization vDC 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 vDC

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

Procedure

1. Type a name and optional description.
2. (Optional) Deselect Enabled.
   - Disabling the Org vDC prevents new vApps from being deployed to the vDC.
3. Click Next.

Confirm Settings and Create the Organization vDC

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

Procedure

1. Review the settings for the organization vDC.
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 vDC network for this vDC.
4. Click Finish to accept the settings and create the organization vDC.
   - When you create an organization vDC, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.
Creating a Published Catalog

You can publish a catalog to make a set of vApp templates or media files available to all of the organizations in a vCloud Director installation.

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

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 Publishing,” on page 41
- “Create a Published Catalog,” on page 42
- “Upload a vApp Template,” on page 42
- “Import a vApp Template from vSphere,” on page 43
- “Upload a Media File,” on page 43
- “Import a Media File from vSphere,” on page 44
- “Publish a Catalog,” on page 44

Enable Catalog Publishing

Before you can publish an organization’s catalogs, you must enable catalog publishing for 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. On the Catalog Publishing tab, select Allow publishing catalogs to all organizations and click OK.
Create a Published Catalog

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

**Prerequisites**

Verify that you have an organization that allows 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 Catalogs and select My Organization's Catalogs in the left pane.
4. On the Catalogs tab, click New.
5. Type a catalog name and optional description and click Next.
6. Click Next.
7. Select Publish to all organizations and click Next.
8. Review the catalog settings and click Finish.

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 OVF 1.0 and OVF 1.1.

vCloud Director supports OVFs based on the Open Virtualization Format (OVF) Specification. If you upload an OVF that includes deployment options, those options are preserved in the vApp template.

You can quarantine files that users upload to vCloud Director so that you can process the files before you accept them. For example, you can scan the files for viruses. See “Quarantine Uploaded Files,” on page 135.

**Prerequisites**

Verify that the following conditions exist:
- The organization to which you are uploading the OVF package has a catalog and an organization vDC.
- 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 Catalogs 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 an organization vDC and 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.

Prerequisites
Verify that you are a vCloud Director 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 Catalogs 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 an organization vDC and catalog.
8. Choose whether to move or copy the virtual machine to the catalog.
9. Choose whether to mark 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.

You can quarantine files that users upload to vCloud Director so that you can process the files before you accept them. For example, you might want to scan the files for viruses. See “Quarantine Uploaded Files,” on page 135.

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 Catalogs 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.
7. Select an organization vDC and 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 Catalogs 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 an organization vDC and catalog.
8. Click OK.

Publish a Catalog

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

**Prerequisites**

Verify that the organization that contains the catalog allows 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 Catalogs 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 Publishing tab, select Publish to all organizations and click OK.

The catalog and all of its contents appear under Public Catalogs for all organizations in the vCloud Director installation.
Managing Cloud Resources

Provider vDCs, organization vDCs, external networks, organization vDC 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 vDCs,” on page 45
- “Managing Organization vDCs,” on page 52
- “Managing External Networks,” on page 64
- “Managing Edge Gateways,” on page 65
- “Managing Organization vDC Networks,” on page 81
- “Managing Network Pools,” on page 94
- “Managing Cloud Cells,” on page 96

Managing Provider vDCs

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

Enable or Disable a Provider vDC

You can disable a provider vDC to prevent the creation of organization vDCs that use the provider vDC resources.

When you disable a provider vDC, vCloud Director also disables the organization vDCs 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 vDC name and select Enable or Disable.
Delete a Provider vDC
You can delete a provider vDC to remove its compute, memory, and storage resources from vCloud Director. The resources remain unaffected in vSphere.

Prerequisites
- Disable the provider vDC.
- Disable and delete all organization vDCs that use the provider vDC.

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

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

Procedure
1. Click the Manage & Monitor tab and click Provider vDCs in the left pane.
2. Right-click the provider vDC 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 vDC, for example, vSphere HA.

Merge Provider vDCs
You can merge two or more provider vDCs into a single provider vDC, combining the resources of all merged provider vDCs.

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

The selected provider vDCs are merged into this provider vDC.

Enable or Disable a Provider vDC 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 vDC 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 vDCs that use its resources.

Prepare or Unprepare a Provider vDC Host

When you add an ESX/ESXi host to a vSphere cluster that vCloud Director uses, you must prepare the host before a provider vDC 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 101.

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 vDC 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 vDCs that use its resources.

Upgrade an ESX/ESXi Host Agent for a Provider vDC 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 vDC 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 vDCs that use the host.

Repair a Provider vDC 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 vDC 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 vDCs that use the host.

**Enable vSphere VXLAN on an Upgraded Provider vDC**

Enable vSphere VXLAN on an upgraded provider vDC to create a VXLAN network pool for the provider vDC. vSphere VXLAN is enabled by default for new provider vDCs.

**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 vDC name and select **Enable VXLAN**.

A VXLAN network pool is created for the provider vDC. See “**VXLAN Network Pools**,” on page 25.

**Provider vDC Datastores**

Provider vDC datastores provide storage capacity for provider vDCs.

**Provider vDC Datastore Metrics**

The following information about each provider vDC datastore appears on the **Datastores** tab of a provider vDC.

**Table 5-1. Datastore Metrics**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the provider vDC datastore.</td>
</tr>
<tr>
<td>Enabled</td>
<td>A checkmark appears when the provider vDC 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 Profile to a Provider vDC

Add a storage profile to a provider vDC to support the storage profile for organization vDCs backed by the provider vDC.

Storage profiles 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 vDC name and select Open.
3. Click the Storage Profiles tab.
4. Click Add Storage Profile.
5. Select a storage profile, click Add and click OK.

Support for the storage profile is added to the provider vDC.

**What to do next**

Configure organization vDCs backed by the provider vDC to support the storage profile. See “Add a Storage Profile to an Organization vDC,” on page 63.

Edit the Metadata for a Storage Profile on a Provider vDC

You can edit the metadata for a storage profile on a provider vDC.

**Procedure**

1. Click the Manage & Monitor tab and click Provider vDCs in the left pane.
2. Right-click the provider vDC name and select Open.
3. Click the Storage Profiles tab.
4. Right-click a storage profile and select Properties.
5. Edit the metadata as appropriate and click OK.

Add a Resource Pool to a Provider vDC

You can add additional resource pools to a provider vDC so that Pay-As-You-Go and Allocation Pool organization vDCs that the provider vDC 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 vDC’s primary resource pool.

**Procedure**

1. Click the Manage & Monitor tab and click Provider vDCs in the left pane.
2. Right-click the provider vDC name and select Open.
3. Click the Resource Pools tab.
5 Select the resource pool to add and click **Finish**.

vCloud Director adds a resource pool for the provider vDC to use, making elastic all Pay-As-You-Go and Allocation Pool organization vDCs backed by the provider vDC.

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 vDC resource pool.

**Enable or Disable a Provider vDC Resource Pool**

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

You must have at least one enabled resource pool on a provider vDC. 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 vDC 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 vDC**

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

**Prerequisites**

1. Disable the resource pool on the provider vDC.
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 vDC 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 vDC**

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

Virtual machines that are part of a reservation pool organization vDC 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 vDC 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 vDC 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 Warnings for a Provider vDC 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 Provider vDCs in the left pane.
2. Right-click the provider vDC 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 vCloud Director sends an email alert, the message indicates which threshold was crossed.
6. Click OK.

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

Send an Email Notification to Provider vDC Users

You can send an email notification to all users who own objects in the provider vDC, 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 vDC name and select Notify.
3 Type the email subject and message and click Send Email.

Managing Organization vDCs

After you create an organization vDC, you can modify its properties, disable or delete it, and manage its allocation model, storage, and network settings.

Create an Organization vDC

Create an organization vDC to allocate resources to an organization. An organization vDC is partitioned from a provider vDC. A single organization can have multiple organization vDCs.

Prerequisites

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

Procedure

1 Open the New Organization vDC Wizard on page 53
   Open the New Organization vDC wizard to start the process of creating an organization vDC.

2 Select an Organization for the Organization vDC on page 53
   You can create an organization vDC to provide resources to any organization in the vCloud Director system. An organization can have more than one organization vDC.

3 Select a Provider vDC on page 53
   An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC 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 vDC compute and memory resources that you allocate are committed to the organization vDC.

5 Configure the Allocation Model on page 56
   Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.

6 Allocate Storage on page 57
   An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC datastores.

7 Select Network Pool and Services on page 58
   A network pool is a group of undifferentiated networks used to create vApp networks and internal organization vDC networks.

8 Configure an Edge Gateway on page 58
   You configure an edge gateway to provide connectivity to one or more external networks.

9 Configure External Networks on page 59
   Select the external networks that the edge gateway can connect to.

10 Configure IP Settings on a New Edge Gateway on page 59
    Configure IP settings for external networks on the new edge gateway.

11 Suballocate IP Pools on a New Edge Gateway on page 59
    Suballocate into multiple static IP pools the IP pools that the external networks on the edge gateway provide.
Configure Rate Limits on a New Edge Gateway on page 59
Configure the inbound and outbound rate limits for each external network on the edge gateway.

Create an Organization vDC Network on page 60
You can create an organization vDC network that is connected to the new edge gateway.

Name the Organization vDC on page 60
You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization vDC.

Confirm Settings and Create the Organization vDC on page 60
Before you create the organization vDC, review the settings you entered.

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

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

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

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

Procedure
1. Select a provider vDC.
   The provider vDC list displays information about available resources and the networks list displays information about networks available to the selected provider vDC.
2. Click Next.
Select an Allocation Model

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

Procedure

1. Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>Only a percentage of the resources you allocate from the provider vDC are committed to the organization vDC. You can specify the percentage for both CPU and memory. This percentage is known as the percentage guarantee factor, and it allows you to overcommit resources. Starting with vCloud Director 5.1, Allocation Pool organization vDCs are elastic by default. This means that the organization vDC spans and utilizes all resource pools associated with its provider vDC. As a result, vCPU frequency is now a mandatory parameter for an Allocation Pool. Set the vCPU frequency and percentage guarantee factor in such a way that a sufficient number of virtual machines can be deployed on the organization vDC without CPU being a bottleneck factor. When a virtual machine is created, the placement engine places it on a provider vDC resource pool that best fits the requirements of the virtual machine. A sub-resource pool is created for this organization vDC under the provider vDC resource pool, and the virtual machine is placed under that sub-resource pool. When the virtual machine powers on, the placement engine checks the provider vDC resource pool to ensure it still has the capacity to power on the virtual machine. If not, the placement engine moves the virtual machine to a provider vDC resource pool with sufficient resources to run the virtual machine. A sub-resource pool for the organization vDC is created if one does not already exist. The sub-resource pool is configured with sufficient resources to run the new virtual machine. The sub-resource 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 vDC. The sub-resource pool’s CPU limit is increased by the number of vCPU the virtual machine is configured with times the vCPU frequency specified at the organization vDC level, and the CPU reservation is increased by the number of vCPU configured for the virtual machine times the vCPU specified at the organization vDC level times the percentage guarantee factor for CPU set at the organization vDC level. The virtual machine is reconfigured to set its memory and CPU reservation to zero and placed. 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 sub-resource pool and that this model can take advantage of new resources added to the provider vDC. In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power on because of a lack of resources on the original resource pool. This might involve a minor cost to move the virtual machine disk files to a new resource pool.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are only committed when users create vApps in the organization vDC. You can specify a percentage of resources to guarantee, which allows you to overcommit resources. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC. Resources committed to the organization are applied at the virtual machine level.</td>
</tr>
</tbody>
</table>
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 there is no sub-resource pool 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.

The benefit of the Pay-As-You-Go model is that it can take advantage of new resources added to the provider vDC.

In rare cases, a virtual machine is switched from the resource pool it was assigned at creation to a different resource pool at power on due to a lack of resources on the original resource pool. This 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 are also unable to take advantage of the resources of idle virtual machines on the same sub-resource pool, since resources are set at the virtual machine level.

All of the resources you allocate are immediately committed to the organization vDC. Users in the organization can control overcommitment by specifying reservation, limit, and priority settings for individual virtual machines.

Because there is only one resource pool and one sub-resource pool 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 very fine control over virtual machine rate, limit, and shares, which can lead to optimal usage of the reserved resources if you plan carefully.

In this model, reservation is always done at the primary cluster. If there are not sufficient resources to create an organization vDC on the primary cluster, the organization vDC creation fails.

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

For information on 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 vDC resources to allocate to the organization vDC.

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

2. Click Next.

Example: Configuring an Allocation Model

When you create an organization vDC, 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

<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 Sub-Resource Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25GHz</td>
<td>CPU Limit</td>
<td>The sum of the number of vCPU times vCPU frequency for all associated virtual machines</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.5GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>The sum of the number of vCPU times vCPU frequency times percentage guarantee for CPU for all associated virtual machines</td>
<td>10GB</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>The 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>The 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 5-3. 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 vDCs always have no reservations or limits. Pay-As-You-Go settings only affect overcommitment. A 100 percent guarantee means no overcommitment is possible. The lower the percentage, the more overcommitment is possible.

Table 5-4. 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>25 GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25GHz, 25GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50GB, 50GB</td>
</tr>
</tbody>
</table>

Allocate Storage

An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC 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 112.

**IMPORTANT** Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider vDC on which the organization vDC is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider vDC on which the organization vDC 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 profile 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 profile used for all virtual machine provisioning operations where the storage profile is not specified.
4. (Optional) Select the Enable thin provisioning check box to enable thin provisioning for virtual machines in the organization vDC.
5. (Optional) Deselect the Enable fast provisioning check box to disable fast provisioning for virtual machines in the organization vDC.
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 vDC 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. Select Manual from the drop-down menu for each external network for which to specify an IP address.
2. 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 vDC Network

You can create an organization vDC 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 vDC network.
3. (Optional) Select Share this network with other vDCs in the organization.
4. Type a gateway address and network mask for the organization vDC 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 vDC

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

Procedure

1. Type a name and optional description.
2. (Optional) Deselect Enabled.
   Disabling the Org vDC prevents new vApps from being deployed to the vDC.
3. Click Next.

Confirm Settings and Create the Organization vDC

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

Procedure

1. Review the settings for the organization vDC.
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 vDC network for this vDC.
4. Click Finish to accept the settings and create the organization vDC.
   When you create an organization vDC, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.
Enable or Disable an Organization vDC

You can disable an organization vDC 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 vDC name and select Enable or Disable.

Delete an Organization vDC

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

Prerequisites

Disable the organization vDC 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 vDC name and select Delete.
3. Click Yes.

Organization vDC Properties

You can edit the properties of an existing organization vDC, including the vDC name and description, allocation model settings, storage settings, and network settings.

- Modify an Organization vDC Name and Description on page 61
  As your vCloud Director installation grows, you might want to assign a more meaningful name or description to an existing organization vDC.
- Edit Organization vDC Allocation Model Settings on page 62
  You cannot change the allocation model for an organization vDC, but you can change some of the settings of the allocation model that you specified when you created the organization vDC.
- Edit Organization vDC Storage Settings on page 62
  After you create and use an organization vDC, you might decide to provide it with more storage resources from its source provider vDC. You can also enable or disable thin provisioning and fast provisioning for the organization vDC.
- Edit Organization vDC Network Settings on page 63
  You can change the maximum number of provisioned networks in an organization vDC and the network pool from which the networks are provisioned.

Modify an Organization vDC Name and Description

As your vCloud Director installation grows, you might want to assign a more meaningful name or description to an existing organization vDC.

Procedure

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Right-click the organization vDC 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 vDC, for example, vSphere HA.

### Edit Organization vDC Allocation Model Settings

You cannot change the allocation model for an organization vDC, but you can change some of the settings of the allocation model that you specified when you created the organization vDC.

#### Procedure

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Right-click the organization vDC 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><strong>CPU allocation</strong></td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization vDC. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td><strong>CPU resources guaranteed</strong></td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization vDC. You can overcommit resources by guaranteeing less than 100%. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td><strong>vCPU Speed</strong></td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization vDC 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><strong>Memory allocation</strong></td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization vDC. This option is available only for Allocation Pool and Reservation Pool allocation models.</td>
</tr>
<tr>
<td><strong>Memory resources guaranteed</strong></td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization vDC. You can overcommit resources by guaranteeing less than 100%. This option is available only for Allocation Pool and Pay-As-You-Go allocation models.</td>
</tr>
<tr>
<td><strong>Maximum number of VMs</strong></td>
<td>Enter the maximum number of virtual machines that can be created in the organization vDC.</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 vDC does not reflect the new settings until all running vApps are stopped and started again.

### Edit Organization vDC Storage Settings

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

Fast provisioning requires vCenter Server 5.0 or later and ESXi 5.0 or later hosts. If the provider vDC on which the organization vDC 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 112.

#### Procedure

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Right-click the organization vDC 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 vDC.

5 (Optional) Select **Enable fast provisioning** to enable fast provisioning for virtual machines in the organization vDC.

6 Click **OK**.

**Edit Organization vDC Network Settings**

You can change the maximum number of provisioned networks in an organization vDC 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 vDC 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 Profile to an Organization vDC**

Add a storage profile to an organization vDC to support the storage profile for virtual machines on the provider vDC.

**Prerequisites**

One or more storage profiles must be associated with the provider vDC that backs the organization vDC. See “**Add a Storage Profile to a Provider vDC**,” on page 49.

**Procedure**

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

2 Double-click the organization vDC name to open the organization vDC.

3 Click the **Storage Profiles** tab and click **Add**.

4 Select a storage profile, click **Add** and click **OK**.

Support for the storage profile is added to the organization vDC.
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.

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, modify the network settings 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.

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, type an IP address or a range of IP addresses in the text box and click Add.
4. Click OK.

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 vDC 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 vDC network with connectivity to external networks and can provide services such as load balancing, network address translation, and a firewall.

Edge gateways require vShield Edge 5.1. For more information, see the vShield documentation.

Add an Edge Gateway

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

Prerequisites

Verify that you are using vShield 5.1.

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 vDC.

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 vDC.

Procedure

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

2. Double-click the organization vDC name to open the organization vDC.

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.</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**.
2. Hold down Ctrl to select multiple networks.
3. Select a network to be the **Default Gateway**.
4. (Optional) Select **Use default gateway for DNS Relay**.
5. 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. Select **Manual** from the drop-down menu for each external network for which to specify an IP address.
2. 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 vDC 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 vDC name to open the organization vDC.
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 vDC that are being sent to another organization vDC 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 vDC name to open the organization vDC.
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 vDC 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 vDC 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 vDC network coming from another organization vDC 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 vDC name to open the organization vDC.
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 vDC 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 69

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 vDC name to open the organization vDC.

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 70.

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 vDC name to open the organization vDC.

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 (Optional) Select Match rule on translated IP to have the rule check against translated IP addresses rather than original IP addresses and choose a traffic direction to apply this rule on.

7 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>

8 Select a Source port to apply this rule on from the drop-down menu.

9 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>

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

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

12 Select the action.

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

13 Select the Enabled check box.

14 (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.

15 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 vDC name to open the organization vDC.

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

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

Click **OK**.

**Enable VPN for an Edge Gateway**

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

vCloud Director supports VPN between organization vDC networks backed by edge gateways and both organization vDC 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 vDC name to open the organization vDC.
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 vDC 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 vDC name to open the organization vDC.
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 vDC networks on the same organization, between organization vDC networks on different organizations, and between an organization vDC 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 vDC Network Backed by an Edge Gateway**

You can create a VPN tunnel between an organization vDC network that is backed by edge gateway and another organization vDC 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 vDC networks in the organization. One of these networks must be backed by the edge gateway. Both organization vDC 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 vDC name to open the organization vDC.
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 vDC 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**

- A routed organization vDC network in each of the organizations. The organization vDC networks must have non-overlapping IP subnets and site-to-site VPN enabled.
- vShield Manager 5.1.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
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 vDC Network Backed by an Edge Gateway to a Remote Network**

You can create a VPN tunnel between an organization vDC 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 vDC 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 vDC name to open the organization vDC.
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 vDC network.
8 Type the peer settings.
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 vDC Network Backed by an Edge Gateway to a Remote Network,” on page 73.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
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 71.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
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 vDC 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 vDC name to open the organization vDC.
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 vDC Network,” on page 89 and “Add Static Routes Between vApp Networks Routed to Different Organization vDC Networks,” on page 90.

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 75
  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 77
  You can delete a server pool from an edge gateway.

- Add a Virtual Server to an Edge Gateway on page 77
  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 78
  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 vDC name to open the organization vDC.
3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Edge Gateway Services**.

4 On the **Load Balancer** tab, click **Pool Servers** and click **Add**.

5 Type a name and optionally a description for the pool server and click **Next**.

6 Click **Enable** for each service to support.

7 Select a balancing method from the drop-down menu for each enabled service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Hash</td>
<td>Selects a server based on a hash of the source and destination IP address of each packet.</td>
</tr>
<tr>
<td>Round Robin</td>
<td>Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server’s processing time remains equally distributed.</td>
</tr>
<tr>
<td>URI</td>
<td>The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down.</td>
</tr>
<tr>
<td>Least Connected</td>
<td>Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.</td>
</tr>
</tbody>
</table>

8 (Optional) Change the default port for each enabled service if necessary.

9 Click **Next**.

10 Change the monitor port if required for each service that is to be supported by this pool.

11 Select the health check mode from the drop-down menu for each service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Tests servers using SSLv3 client hello messages. The server is considered valid only when the response contains server hello messages.</td>
</tr>
<tr>
<td>HTTP</td>
<td>The GET / default method is used to detect server status. Only responses 2xx and 3xx are valid. Other responses (including a lack of response) indicate a server failure.</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP connection check.</td>
</tr>
</tbody>
</table>

12 (Optional) Change the default health check parameters if necessary.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Interval at which a server is pinged.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time within which a response from the server must be received.</td>
</tr>
<tr>
<td>Health Threshold</td>
<td>Number of consecutive successful health checks before a server is declared operational.</td>
</tr>
<tr>
<td>Unhealth Threshold</td>
<td>Number of consecutive unsuccessful health checks before a server is declared dead.</td>
</tr>
</tbody>
</table>

13 For HTTP, type the URI referenced in the HTTP ping requests.

14 Click **Next**.

15 Click **Add** to add a back-end server to the pool.

16 Type the IP address of the server.

17 Type the weight to indicate the ratio of how many requests are to be served by this back-end server.

18 Change the default port and monitor port for the server if required.
19. Click OK.

20. (Optional) Repeat Step 15 through Step 19 to add additional servers.

21. Click Next.

22. Verify that the settings for the pool server are correct and click Finish.

**Edit Pool Server Settings**

You can edit the settings of an existing pool server.

**Prerequisites**

There must be an existing pool server on the edge gateway. See “Add a Pool Server to an Edge Gateway,” on page 75.

**Procedure**

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
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 75.

**Procedure**

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
On the Load Balancer tab, click Virtual Servers and click Add.

Type a name for the virtual server.

(Optional) Type a description for the virtual server.

Select an external network from the Applied on drop-down menu.

Type the IP address of the virtual server.

Select a pool from the drop-down menu to be associated with the virtual server.

In Services, select Enable for each service to be supported.

Change the default Port, Persistence Method, Cookie Name, and Cookie Mode values for each enabled service as required.

Click Enabled to enable the virtual server.

(Optional) Click Log network traffic for virtual server.

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 77.

Procedure

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
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 vDC name to open the organization vDC.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
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.
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 vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
3 Click the **Edge Gateways** tab, right-click the edge gateway name, and select **Properties**.
4 Click the **Configure IP Settings** tab.
5 Type a new IP address for each external network to modify, 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 vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
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**.

### Delete an Edge Gateway

You can delete an edge gateway to remove it from the organization vDC.

**Prerequisites**

Delete any organization vDC 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 vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
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 vDC name to open the organization vDC.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Synchronize syslog server settings.
4. Click Yes.

Managing Organization vDC Networks

System administrators and organization administrators can add, delete, and modify routed and isolated organization vDC networks. Only a system administrator can add, delete, and modify a direct organization vDC network.

Adding Networks to an Organization vDC

Add a network to an organization vDC to enable its virtual machines to communicate with each other or to provide access to the Internet. A single organization vDC can have multiple networks.
<table>
<thead>
<tr>
<th>Organization vDC Network Type</th>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>External organization vDC 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 vDC 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 Org vDC Networks tab, NAT-routed networks display a gateway address.</td>
<td>vSphere Edge 5.1 and an edge gateway</td>
</tr>
<tr>
<td>Internal organization vDC 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. Machines outside of this organization have no connectivity to machines within the organization. On the Org vDC Networks tab, internal networks do not display an associated gateway address.</td>
<td>Network pool</td>
</tr>
</tbody>
</table>

### Create an External Direct Organization vDC Network

You can create an external direct organization vDC 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 vDC name to open the organization vDC.
3. Click the Org vDC Networks tab and click Add Network.
4. Select Connect directly to an external network.
5. Select an external network and click Next.
6. Type a name and optional description.
7. (Optional) Select Share this network with other vDCs in the organization to make the organization vDC network available to other organization vDCs in the organization.
8. Click Next.
9 Review the settings for the organization vDC network.
   Click Finish to accept the settings and create the organization vDC network, or click Back to modify the settings.

Create an External Routed Organization vDC Network
You can create an external routed organization vDC network that only this organization can access.

Prerequisites
Verify that you have vShield Edge 5.1 and an edge gateway on your organization vDC.

Procedure
1 Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2 Double-click the organization vDC name to open the organization vDC.
3 Click the Org vDC Networks tab and click Add Network.
4 Select Create a routed network by connecting to an existing edge gateway.
5 Select an edge gateway and click Next.
6 Type a Gateway address and Network mask for the organization vDC 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 vDC network available to other organization vDCs in the organization.
13 Click Next.
14 Review the settings for the organization vDC network.
   Click Finish to accept the settings and create the organization vDC network, or click Back to modify the settings.

Create an Internal Organization vDC Network
You can create an internal organization vDC 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 vDC name to open the organization vDC.
3 Click the Org vDC Networks tab and click Add Network.
4 Select Create an isolated network within this virtual datacenter and click Next.
5 Type a **Gateway address** and **Network mask** for the organization vDC 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 vDC network available to other organization vDCs in the organization.

12 Click **Next**.

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

An organization vDC network is created.

### Configuring Organization vDC Network Services

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

Table 5-6 lists the network services that vCloud Director provides to each type of organization vDC network.

<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 vDC network - direct connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External organization vDC network - routed connection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internal organization vDC network</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configure DHCP for an Organization vDC Network

You can configure certain organization vDC 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 vDC 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 vDC network or an internal organization vDC network.

#### Procedure

1 Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2 Double-click the organization vDC name to open the organization vDC.

3 Click the **Org vDC Networks** tab, right-click the organization vDC 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 vDC 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 vDC Network

You can configure certain organization vDC networks to provide firewall services. You can enable the firewall on an organization vDC 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 vDC Network,” on page 85.

System administrators and organization administrators can enable firewalls.

#### Prerequisites

Verify that you have an external routed organization vDC network.

#### Procedure

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

2 Double-click the organization vDC name to open the organization vDC.

3 Click the **Org vDC Networks** tab, right-click the organization vDC 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 vDC Network

You can add firewall rules to an organization vDC 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 vDC network. See “Enable the Firewall for an Organization vDC Network,” on page 85.

When you add a new firewall rule to an organization vDC 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 vDC Network,” on page 86.

System administrators and organization administrators can add firewall rules.
Prerequisites
Verify that you have an external NAT-routed organization vDC network.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC network.
8. Type the destination IP address and select the destination port.
   For incoming traffic, the destination is the organization vDC 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 vDC 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 vDC 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 vDC 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 vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC Network

You can enable VPN for an organization vDC network and create a secure tunnel to another network. vCloud Director supports VPN between organization vDC networks in the same organization, organization vDC networks in different organizations (including organization vDC networks in different instances of vCloud Director), and remote networks.

System administrators and organization administrators can enable VPN.

Prerequisites
- An external routed organization vDC network.
- vShield Manager 5.1.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name, and select Configure Services.
4. Click the VPN tab and select Enable VPN.
5. (Optional) Type a public IP address.
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 vDC 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
- At least two routed organization vDC networks with non-overlapping IP subnets and VPN enabled on both networks.
- vShield Manager 5.1.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC 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**

- A routed organization vDC network and a routed remote network that uses IPSec.
- vShield Manager 5.1.

**Procedure**

1. Click the **Manage & Monitor** tab and click **Organization vDCs** in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the **Org vDC Networks** tab, right-click the organization vDC 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 vDC Network**

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

**Prerequisites**

Verify that you have a routed organization vDC network.
Procedure

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC Network,” on page 89 and “Add Static Routes Between vApp Networks Routed to Different Organization vDC Networks,” on page 90.

Add Static Routes Between vApp Networks Routed to the Same Organization vDC Network

You can add static routes between two vApp networks that are routed to the same organization vDC 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 vDC 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 Manager 5.1 is installed.
- A routed organization vDC network.
- Static routing is enabled on the organization vDC network.
- Two vApp networks are routed to the organization vDC 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 vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC network to allow traffic between the vApp networks. You can use information about the vApp networks to create the static routes.

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network Specification</th>
<th>Router External IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>192.168.2.0/24</td>
<td>192.168.0.101</td>
</tr>
<tr>
<td>Org vDC Network Shared</td>
<td>192.168.0.0/24</td>
<td>NA</td>
</tr>
</tbody>
</table>

On Org vDC Network Shared, create a static route to vApp Network 1 and another static route to vApp Network 2.

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network Specification</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 vDC Network,” on page 85.

**Add Static Routes Between vApp Networks Routed to Different Organization vDC Networks**

An organization administrator can add static routes between two vApp networks that are routed to different organization vDC 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 vDC 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:

- vShield Manager 5.1.
- Two organization vDC networks routed to the same external network.
- Static routing is enabled on both organization vDC networks.
A vApp network is routed to each organization vDC 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 vDC name to open the organization vDC.
3. Click the **Org vDC Networks** tab, right-click the organization vDC 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 vDC 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 vDC 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 vDC 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 vDC networks to allow traffic between the vApp networks. You can use information about the vApp networks and organization vDC networks to create the static routes.

**Table 5-9: 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>192.168.11.0/24</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 5-10: Static Routing Settings for Org vDC Network 1**

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network Specification</th>
<th>Next Hop IP Address</th>
<th>Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 2</td>
<td>tovapp2</td>
<td>192.168.11.0/24</td>
<td>10.112.205.100</td>
<td>To external network</td>
</tr>
<tr>
<td>vApp Network 1</td>
<td>tovapp1</td>
<td>192.168.1.0/24</td>
<td>192.168.0.100</td>
<td>Within this network</td>
</tr>
</tbody>
</table>
Table 5-11. Static Routing Settings for Org vDC Network 2

<table>
<thead>
<tr>
<th>Static Route to Network</th>
<th>Route Name</th>
<th>Network</th>
<th>Next Hop IP Address</th>
<th>Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp Network 1</td>
<td>tovapp1</td>
<td>192.168.1.0/24</td>
<td>10.112.205.101</td>
<td>To external network</td>
</tr>
<tr>
<td>vApp Network 2</td>
<td>tovapp2</td>
<td>192.168.11.0/24</td>
<td>192.168.10.100</td>
<td>Within this network</td>
</tr>
</tbody>
</table>

What to do next

Create firewall rules to allow traffic on the static routes. See “Add a Firewall Rule for an Organization vDC Network,” on page 85.

Reset an Organization vDC Network

If the network services that are associated with an organization vDC 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 vDC, reset the organization vDC networks that depend on it.

No network services are available while an organization vDC network resets.

Prerequisites

Verify that you have a routed organization vDC network or an internal organization vDC network.

Procedure

1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name, and select Reset Network.
4. Click Yes.

View vApps and vApp Templates That Use an Organization vDC Network

You can view a list of the all the vApps and vApp templates that include virtual machines with a NIC connected to an organization vDC network. You cannot delete an organization vDC 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 vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name and select Connected vApps.
4. Click OK.

Delete an Organization vDC Network

You can delete an organization vDC network to remove it from the organization vDC.

Prerequisites

Verify that no virtual machines are connected to the organization vDC network. See “View vApps and vApp Templates That Use an Organization vDC Network,” on page 92.
Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name, and select Delete.

View IP Use for an Organization vDC Network
You can view a list of IP addresses that are currently in use in an organization vDC network IP pool.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name, and select IP Allocations.

Editing Organization vDC Network Properties
You can edit the properties of an existing organization vDC network, including the network name and description, IP addresses, and DNS settings.

- Add IP Addresses to an Organization vDC Network IP Pool on page 93
  If an organization vDC network is running out of IP addresses, you can add more addresses to its IP Pool.
- Modify an Organization vDC Network Name and Description on page 94
  As your vCloud Director installation increases, you might want to assign a more descriptive name or description to an existing organization vDC network.
- Modify an Organization vDC Network DNS Settings on page 94
  You can change the DNS settings for certain types of organization vDC networks.

Add IP Addresses to an Organization vDC Network IP Pool
If an organization vDC network is running out of IP addresses, you can add more addresses to its IP Pool.

Prerequisites
Verify that you have a routed organization vDC network or an internal organization vDC network.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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 vDC 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 vDC network.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC network name, and select Properties.
4. Type a new name and optional description and click OK.

Modify an Organization vDC Network DNS Settings
You can change the DNS settings for certain types of organization vDC networks.

Prerequisites
Verify that you have a routed organization vDC network or an internal organization vDC network.

Procedure
1. Click the Manage & Monitor tab and click Organization vDCs in the left pane.
2. Double-click the organization vDC name to open the organization vDC.
3. Click the Org vDC Networks tab, right-click the organization vDC 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.

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.

**Prerequisites**

Verify that the following conditions exist:

- No organization vDC is associated with the network pool.
- No vApps use the network pool
- No organization vDC 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 5-12 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 96.

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 `/opt/vmware/vcloud-director/bin/vmware-vcd-cell stop` command.
2. Start the cell by running the `service vmware-vcd start` command.

Users can now access the cell by using a browser or the vCloud API.
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 99
- “Managing vSphere ESX/ESXi Hosts,” on page 101
- “Managing vSphere Datastores,” on page 102
- “Managing Stranded Items,” on page 103

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 On the General tab, type the new settings and click **OK**.

**Reconnect a vCenter Server**

If vCloud Director loses it connection to a vCenter Server, or if you change the connection settings, you can try to reconnect.

**Procedure**
1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.
2 Right-click the vCenter Server name and select **Reconnect vCenter**.
3 Read the informational message and click **Yes** to confirm.

**Enable or Disable a vCenter Server**

You can disable a vCenter Server to perform maintenance.

**Procedure**
1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.
2 Right-click the vCenter Server name and select **Disable** or **Enable**.
3 Click **Yes**.

**Remove a vCenter Server**

You can remove a vCenter Server to stop using its resources with vCloud Director.

**Prerequisites**

Before you can remove a vCenter server, you must disable it and delete all of the provider vDCs 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**.
What to do next
Register vCloud Director with the upgraded server. See “Register vCloud Director with a vCenter Server,” on page 99.

Modify vShield Manager Settings
If the connection settings for the vShield Manager for a vCenter Server change, or if you want to use a different vShield Manager, 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 Manager 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 vDCs 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 vDC 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 101.

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 vDCs 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 vDC. 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 vDCs that use its resources.

**Remove a Datastore**

You can remove a datastore from vCloud Director to prevent provider vDCs from using its storage resources.

**Prerequisites**

Verify that the datastore is disabled and removed from all of the provider vDCs that use it.

**Procedure**

1 Click the **Manage & Monitor** tab and click **Datastores** in the left pane.
2 Right-click the datastore name and select **Remove**.
3 Click **Yes**.

vCloud Director removes the datastore.

**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.

**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 104.

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 103.

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.
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 105
- “Delete an Organization,” on page 105
- “Add a Catalog to an Organization,” on page 106
- “Editing Organization Properties,” on page 106
- “Managing Organization Resources,” on page 110
- “Managing Organization Users and Groups,” on page 110
- “Managing Organization vApps and Virtual Machines,” on page 110

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 or change ownership of all objects that the organization users own.

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 107
  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 107
  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 107
  You can use an LDAP service to provide a directory of users and groups to import into an organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.

- **Modify Organization Catalog Publishing Policy** on page 108
  A catalog provides organization users with a library of vApp templates and media that they can use to create vApps. Generally, catalogs should only be available to users in a single organization, but a system administrator can allow the organization administrator to publish a catalog to all organizations in the vCloud Director installation.

- **Modify Organization Email Preferences** on page 108
  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 123.

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>
</tbody>
</table>
| VCD system LDAP service       | (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.  
Note: 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. |
| Custom LDAP service           | Click the Custom LDAP tab, type the custom LDAP settings for the organization, and click OK. |

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 Publishing Policy

A catalog provides organization users with a library of vApp templates and media that they can use to create vApps. Generally, catalogs should only be available to users in a single organization, but a system administrator can allow the organization administrator to publish a catalog to all organizations in the vCloud Director installation.

**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 Publishing 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</td>
<td>Organization administrator can publish a catalog for users in all organizations.</td>
</tr>
<tr>
<td>all organizations</td>
<td></td>
</tr>
</tbody>
</table>

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

### 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 27.

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.
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 vDCs. If an organization needs more resources, you can add a new organization vDC or modify an existing organization vDC. You can take resources away from an organization by removing or modifying an organization vDC.

For more information about adding an organization vDC, see “Create an Organization vDC,” on page 52. For information about removing an organization vDC, see “Delete an Organization vDC,” on page 61. For information about modifying the resources available to an existing organization vDC, see “Edit Organization vDC Allocation Model Settings,” on page 62, and “Edit Organization vDC Storage Settings,” on page 62.

Managing Organization Users and Groups

When you create an organization, you can add one or more local users to the organization. After you create the organization, you, or an organization administrator, can add local users, LDAP users, and LDAP groups to the organization.

For more information about adding users and groups to an organization, see the VMware vCloud Director User’s Guide.

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 vDC.

Procedure

1. Click the Manage & Monitor tab and click Organizations in the left pane.
2. Right-click the organization name and select Open.
3. Click the My Cloud tab and click vApps in the left pane.
4. Right-click the vApp name and select Open.
5. On the Virtual Machines tab, click the Actions button and select Import from vSphere.
6. Select a vCenter Server and a virtual machine.
7. Type a name and optional description for the virtual machine.
8. Select whether to copy or move the source virtual machine.
9. Click OK.
Create a vApp Based on a vSphere Virtual Machine

A system administrator can import a vSphere virtual machine to an organization as a vCloud Director vApp.

**Prerequisites**

Verify that you are logged in to vCloud Director as a system administrator and that the organization has an available organization vDC.

**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 vDC.
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 112.

Fast provisioning is enabled by default on organization vDCs. Fast provisioning requires vCenter 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains ESX/ESXi 4.x hosts, you must disable fast provisioning. See “Edit Organization vDC Storage Settings,” on page 62.

**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 112.

**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 113
- “Import a System Administrator,” on page 113
- “Enable or Disable a System Administrator,” on page 114
- “Delete a System Administrator,” on page 114
- “Edit System Administrator Profile and Contact Information,” on page 114
- “Send an Email Notification to Users,” on page 115
- “Delete a System Administrator Who Lost Access to the System,” on page 115
- “Import a Group,” on page 115
- “Delete an LDAP Group,” on page 116
- “View Group Properties,” on page 116
- “Roles and Rights,” on page 116

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 129.
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.

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 users from an LDAP server.</td>
</tr>
<tr>
<td></td>
<td>a Type a full or partial name in the text box and click Search Users.</td>
</tr>
<tr>
<td></td>
<td>b Select the users to import and click Add.</td>
</tr>
<tr>
<td>vSphere SSO</td>
<td>Import users from vCenter Single Sign On. Type the user names of the users to import and click Add. Separate multiple users with carriage returns.</td>
</tr>
</tbody>
</table>

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 113 and “Import a System Administrator,” on page 113.

**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 129.

**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</td>
</tr>
<tr>
<td></td>
<td>and 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 115.

**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 137.

- **Create a Role** on page 117
  
  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 117
  
  To create a role based on an existing role, you can copy a role and modify its rights.
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 119
- “General System Settings,” on page 119
- “Editing System Email Settings,” on page 121
- “Configuring Blocking Tasks and Notifications,” on page 122
- “Configuring the System LDAP Settings,” on page 123
- “Customize the vCloud Director Client UI,” on page 126
- “Configuring Public Addresses,” on page 127
- “Configure the Account Lockout Policy,” on page 129
- “Configure vCloud Director to use vCenter Single Sign On,” on page 129

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 119.

Procedure

1. Click the Administration tab and click General in the left pane.
2. Modify the settings and click Apply.

General System Settings

vCloud Director includes general system settings that you can modify to meet your needs.

Table 9-1. General System Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Start Time</td>
<td>LDAP Synchronization</td>
<td>Time of day to start LDAP synchronization.</td>
</tr>
<tr>
<td>Synchronization Interval</td>
<td>LDAP Synchronization</td>
<td>The number of hours between LDAP synchronisations.</td>
</tr>
<tr>
<td>Login policy</td>
<td>Login Policy</td>
<td>Select a login policy.</td>
</tr>
</tbody>
</table>
Table 9-1. General System Settings (Continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 (for example, VMware vShield Manager) 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>Miscellaneous</td>
<td>Amount of time the vCloud Director application remains active without user interaction.</td>
</tr>
<tr>
<td>Maximum session timeout</td>
<td>Miscellaneous</td>
<td>Maximum amount of time the vCloud Director application remains active.</td>
</tr>
<tr>
<td>Host refresh frequency</td>
<td>Miscellaneous</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>Miscellaneous</td>
<td>Select the amount of time to wait before marking a host as hung.</td>
</tr>
<tr>
<td>Transfer session timeout</td>
<td>Miscellaneous</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>Chargeback Event History to Keep</td>
<td>Miscellaneous</td>
<td>Number of days of chargeback event history to keep before deleting it.</td>
</tr>
<tr>
<td>Chargeback Event Cleanup Start Time</td>
<td>Miscellaneous</td>
<td>Time of day to start chargeback event history cleanup.</td>
</tr>
<tr>
<td>Provide default vApp names</td>
<td>Miscellaneous</td>
<td>Select the check box to generate default names for vApps.</td>
</tr>
<tr>
<td>Enable upload quarantine with a timeout of _ seconds</td>
<td>Miscellaneous</td>
<td>Select the check box and enter a timeout number representing the amount of time to quarantine uploaded files. For more information about working with quarantined files, see “Monitoring Quarantined Files,” on page 135.</td>
</tr>
<tr>
<td>Verify vCenter certificates</td>
<td>Miscellaneous</td>
<td>Select the check box to allow vCloud Director to communicate only with trusted vCenter servers. Click <strong>Browse</strong> to locate the JCEKS keystore and type the keystore password.</td>
</tr>
</tbody>
</table>
Editing System Email Settings

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

- **Configure SMTP Settings** on page 121
  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 121
  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.

**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** | **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 the keystore password.

   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**.
8. Type a user name and password to connect to the AMQP host.
9. Click Test AMQP Connection to test the settings.
10. Click Apply.

(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>
<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>
</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 125.

Procedure

1. Click the Administration tab and click LDAP in the left pane.
2. Type the host name or IP address of the LDAP server.
   - For Kerberos authentication, use the fully qualified domain name (FQDN).
3. Type a port number.
   - For LDAP, the default port number is 389. For LDAP over SSL (LDAPS), the default port number is 636.
4. Type the base distinguished name (DN).
   - The base DN is the location in the LDAP directory where vCloud Director connects. VMware recommends connecting at the root. Type the domain components only, for example, DC=example, DC=com.
   - To connect to a node in the tree, type the distinguished name for that node, for example, OU=ServiceDirector, DC=example, DC=com. Connecting to a node limits the scope of the directory available to vCloud Director.
5. Select the SSL check box to use LDAPS and choose one of the certificate options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept all certificates</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Click <strong>Browse</strong> to locate the SSL certificate.</td>
</tr>
<tr>
<td>SSL Keystore</td>
<td>Click <strong>Browse</strong> to locate the SSL keystore. Type and confirm the keystore password.</td>
</tr>
</tbody>
</table>
6. Select an authentication method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Simple authentication consists of sending the LDAP server the user's DN and password. If you are using LDAP, the LDAP password is sent over the network in clear text.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos issues authentication tickets to prove a user's identity. If you select Kerberos, you must select a realm.</td>
</tr>
</tbody>
</table>
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>

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 119.

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 128
   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 128
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 128
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.
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. Type the URL of the vCloud Director you are configuring, and 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 113 and “Import a Group,” on page 115.
System administrators can monitor completed and in-progress operations and view resource usage information at the provider vDC, organization vDC, and datastore level.

This chapter includes the following topics:

- “Viewing Tasks and Events,” on page 131
- “Monitor and Manage Blocking Tasks,” on page 133
- “View Usage Information for a Provider vDC,” on page 133
- “View Usage Information for an Organization vDC,” on page 133
- “Using vCloud Director's JMX Service,” on page 134
- “Viewing the vCloud Director Logs,” on page 134
- “vCloud Director and Cost Reporting,” on page 134
- “Monitoring Quarantined Files,” on page 135

### Viewing Tasks and Events

You can view system tasks and events and organization tasks and events to monitor and audit vCloud Directory activities.

vCloud Director tasks represent long-running operations and their status changes as the task progresses. For example, a task's status generally starts as Running. When the task finishes, its status changes to Successful or Error.

vCloud Director events represent one-time occurrences that typically indicate an important part of an operation or a significant state change for a vCloud Director object. For example, vCloud Director logs an event when a user initiates the creation an organization vDC 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 132.

The log can also include debug information, depending on your vCloud Director settings. See “General System Settings,” on page 119.
**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 131.

The log can also include debug information, depending on your vCloud Director settings. See “General System Settings,” on page 119.

**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 132.

**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 132.
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 Error.</td>
</tr>
</tbody>
</table>
3. Type a reason and click OK.

View Usage Information for a Provider vDC
Provider vDCs supply compute, memory, and storage resources to organization vDCs. You can monitor provider vDC 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 vDC.

View Usage Information for an Organization vDC
Organization vDCs supply compute, memory, and storage resources to organizations. You can monitor organization vDC 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 vDC.
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.

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 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 cell crashes, is restarted, and so on</td>
</tr>
<tr>
<td>diagnostics.log</td>
<td>Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.</td>
</tr>
<tr>
<td>YYYY_MM_DD.request.log</td>
<td>HTTP request logs in the Apache common log format.</td>
</tr>
</tbody>
</table>

You can use any text editor/viewer or third-party tool to view the logs.

vCloud Director and Cost Reporting

You can use VMware vCenter Chargeback 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 119.

Monitoring Quarantined Files

vCloud Director allows you to quarantine files (vApp templates and media files) that users upload to the system. You can enable upload quarantine and use third-party tools (for example, a virus scanner) to process uploaded files before vCloud Director accepts them.

You can use any Java Message Service (JMS) client that understands the STOMP protocol to monitor and respond to messages from the vCloud Director quarantine service.

When an uploaded file is quarantined, a JMS broker sends a message to a request queue on a cloud cell. The receiver decides whether to accept or reject the upload by sending a message to a response queue.

Quarantine Uploaded Files

You can quarantine files that users upload to vCloud Director so that you can process the files (for example, scan them for viruses) before accepting them.

Procedure

1. Click the Administration tab and click General in the left pane.
2. Select the Enable upload quarantine checkbox and type a timeout in seconds.
   The timeout represents the amount of time to quarantine uploaded files before deleting them.
3. Click Apply.

vApp templates and media files that users upload are not available for use until they are accepted.

What to do next

Set up a manual or automatic system to listen for, process, and respond to quarantine service messages.

View Quarantine Requests Using JConsole

You can use JConsole to view quarantine service requests. You will use the information in the request message to construct a response message.

Prerequisites

Upload quarantine is enabled.

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 and browse to the org.apache.activemq > uuid > Queue > com.vmware.vcloud.queues.transfer.server.QuarantineRequest > Operations node.
6. Select the browseMessages() operation.
Copy the text of the message to which you want to respond.

For example,

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<QuarantineRequestMessage transferSessionId="239d310a-5bce-492d-9e26-ed6b646dc15"
transferSessionFilePath="/opt/vmware/vcloud-director/data/transfer/239d310a-5bce-492d-9e26-ed6b646dc15"
xmlns="http://www.vmware.com/vcloud/v1"/>
```

**What to do next**

Accept or reject the quarantine request.

**Accept or Reject a Quarantine Request Using JConsole**

You can use JConsole to accept or quarantine service requests. You will need the information in the request message to construct a response message.

**Prerequisites**

You have the text of the request message.

**Procedure**

1. Paste the text of the request message into a text editor.
2. Change the XML element name to QuarantineResponseMessage and add a new attribute to the element, `response="accept"` or `response="reject"`.
   
   For example,
   ```xml
   <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
   <QuarantineResponseMessage transferSessionId="239d310a-5bce-492d-9e26-ed6b646dc15"
   transferSessionFilePath="/opt/vmware/vcloud-director/data/transfer/239d310a-5bce-492d-9e26-ed6b646dc15"
   response="accept"
   xmlns="http://www.vmware.com/vcloud/v1"/>
   ```
4. In the Connection menu, select **New Connection**.
5. 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.
6. Type a vCloud Director system administrator user name and password and click **Connect**.
7. Click the MBeans tab and browse to the `org.apache.activemq > uuid > Queue > com.vmware.vcloud.queues.transfer.server.QuarantineResponse > Operations` node.
8. Select the `sendTextMessage(string, string, string)` operation.
9. Paste the response message from your text editor in the first field and type a vCloud Director system administrator user name and password in the other fields.
10. Click **sendTextMessage**.

For an accepted file, vCloud Director releases the file from quarantine and completes the upload. For a rejected file, vCloud Director removes the file.
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.
A system administrator can create new roles and modify existing roles, except the System Administrator role.

Table 11-1. Default Rights for the Predefined Roles

<table>
<thead>
<tr>
<th></th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp: Create/Reconfigure a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Delete a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Edit vApp Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Start/Stop/Suspend/Reset a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Share a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Copy a vApp</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vApp: Access to VM Console</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Role</td>
<td>System Administrator</td>
<td>Organization Administrator</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>
<td>---------------------</td>
</tr>
<tr>
<td>vApp: Change Owner</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Memory</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM CPU</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Network</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Edit VM Hard Disk</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp: Manage VM Password Settings</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Create/Delete a new Catalog</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Edit Catalog Properties</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Add a vApp from My Cloud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Publish a Catalog</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Share a Catalog</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View Private and Shared Catalogs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: View Published Catalogs</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog: Change Owner</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Edit vApp Template/Media Properties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Create/Upload a vApp Template or Media</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Item: Download a vApp Template</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 11-1. Default Rights for the Predefined Roles (Continued)

<table>
<thead>
<tr>
<th>Catalog Item: Copy/Move a vApp Template or Media</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Catalog Item: View vApp Templates and Media</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Catalog Item: Add to My Cloud</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit Organization Properties</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit SMTP Settings</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit Quotas Policy</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: View Organizations</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit vDC Network Properties</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: View vDC Networks</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit Leases Policy</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: Edit Password Policy</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization: View Organization vDCs</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User: View Group/User</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General: Send Notification</th>
<th>System Administrator</th>
<th>Organization Administrator</th>
<th>Catalog Author</th>
<th>vApp Author</th>
<th>vApp User</th>
<th>Console Access Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>System Administrator</td>
<td>Organization Administrator</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>
<td>---------------------</td>
</tr>
<tr>
<td>General: Administrator</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General: Administrator</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Index

## A
- account lockout 129
- activity log 131, 132
- adding resources 19
- adding vSphere resources 19
- allocation models 34, 36, 54, 56
- allocation pool allocation model 34, 54
- AMQP broker 122

## B
- blocking tasks
  - about 122
  - configuring settings 122
  - configuring tasks 123
- branding the UI
  - revert to system logo 127
  - revert to system theme 127

## C
- catalog publishing, enabling 41
- catalogs
  - adding 106
  - creating 42
- publishing 41, 44
- certificates, replacing 16
- changing your password 17
- Cisco Nexus 1000V 24
- cloud cells
  - adding 96
  - deleting 96
- maintenance message 96, 97
- managing 96
- restarting 96
- starting 96
- stopping 96
- cloud resources 21, 45
- cost reporting 134

## D
- datastores
  - disk space warnings 51, 103
  - enabling and disabling 102
  - monitoring capacity 51
  - removing 103
- DHCP network services 67, 84

## E
- edge gateway
  - add 38, 58, 67
- adding 65
- adding a firewall rule 69
- apply syslog server settings 81
- configuring DHCP 67
- configuring firewalls 69
- create VPN tunnel 71, 73
- deleting 80
- description 67
- DNS 39, 59, 66, 79
- enabling site-to-site VPN 71
- enabling static routing 75
- external networks 39, 59, 66, 79
- gateway configuration 38, 58, 66
- HA 79
- high availability 79
- IP address 39, 59, 66, 79
- IP pools 39, 59, 66, 80
- load balancing 75
- name 67
- ordering firewall rules 70
- organization vDC 66
- properties 78
- rate limits 39, 59, 67, 80
- services 67
- viewing IP usage 81
- elastic vDC 34, 49, 54
- email notifications 51, 115, 121
- email settings 121
- ESX/ESXi hosts
  - enabling and disabling 46, 101
  - moving virtual machines 101
  - preparing and unpreparing 47, 102
  - repairing 47, 102
- upgrading agent 47, 102
- extensions
  - aborting 133
  - configuring AMQP 122
  - failing 133
  - resuming 133
- external networks
  - adding 22
  - adding IP addresses 64
defined 22
deleting 64
name and description 64
specification 64

F
fast provisioning 37, 57, 62, 112
firewall rules, setting the order 70, 86

G
general system settings 119
going started 11
groups, view 116
guest customization, preparing 14, 15
guided tasks 14

I
identity provider 129
importing
media files 44
vApp templates 43

J
JMX, accessing 134
JMX service 134

K
Kerberos realm 125

L
LDAP
configuring 123
customizing attributes 126
setting up the connection 124
support 123
synchronizing 126
testing the connection 125
leases, runtime and storage 27
licensing, vShield 21
linked clones 112
load balancer 128
load balancing
pool servers 75, 77
server pools 77
virtual servers 77, 78
logging in 13
logs 134
Lost & Found 115

M
MBeans 134
media, uploading 43
Microsoft Sysprep 14, 15
monitoring, tasks and events 131
monitoring vCloud Director 131
MTU 25

N
NAT 68
Network Address Translation 68
network pools
adding Cloud isolated networks 95
adding port groups 94
adding VLAN IDs 95
cloud network isolation-backed 23
defined 23
deleting 95
name and description 94
port group-backed 24
setting the MTU 25
VLAN-backed 23
VXLAN 25
network quota 38, 58
network services 84
Nexus 1000V 24
notifications, about 122

O
organization vDC networks
adding a firewall rule 85
adding a static route 89, 90
adding IP addresses 93
configuring DHCP 84
configuring firewalls 85
configuring services 84
connected vApp templates 92
connected vApps 92
create VPN tunnel 72, 87, 88
creating 40, 60, 81
deleting 92
enabling site-to-site VPN 87
enabling static routing 88
external direct 82
external NAT-routed 83
internal 83
managing 81
modifying DNS 94
modifying the name and description 94
ordering firewall rules 86
properties 93
resetting 92
viewing IP usage 93
organization vDCs
allocating storage 37, 57
allocation model settings 62
allocation models 36, 56
changing description 61
changing name 61
confirm settings 40, 60
creating 33, 52, 53
deleting 61
enabling or disabling 61
monitoring usage 133
naming 40, 60
network pools 63
network quota 38, 58
properties 61
selecting a network pool 38, 58
selecting a provider vDC 33, 53
selecting the organization 53
storage capacity 62
organizations
adding local users 30
allocating resources 32, 33
catalog publishing 108
confirm settings 31
creating 28
deleting 105
email preferences 30, 108
enabling or disabling 105
full name and description 107
LDAP options 29, 107
lease settings 31, 109
limit settings 31, 109
managing 105
managing resources 110
monitoring events 132
monitoring tasks 132
naming 29
properties 106
publishing catalogs 30
quota settings 31, 109
renaming 107
SMTP server 30
SMTP settings 108
users and groups 110
vApps 110
OVF upload 42

P
password policy 129
pay-as-you-go allocation model 34, 54
peer settings 74
pool servers
add 75
edit 77
settings 77
provider vDCs
adding resource pools 49
changing name 46
creating 21
datastores 48
defined 21
deleting 46
enabling or disabling 45
management 45
monitoring usage 133
Provider vDCs, merging 46
public addresses 127
public IP address 71
publishing catalogs 41, 44
Q
quarantine service
accepting requests 136
enabling 135
overview 135
rejecting requests 136
viewing requests 135
quick start tasks 14
R
reservation pool allocation model 34, 54
resource pools
detach 50
disable 50
enable 50
roles
copying 117
creating 117
deleting 117
editing 117
roles and rights 137
runtime leases 27
S
server pools, delete 77
shadow virtual machines 112
single sign-on 129
SMTP server 108
SMTP settings 121
SSO 129
storage leases 27
storage profiles
add 49, 63
name 49
type 49
value 49
stranded items
deleting 103
force deleting 104
system
monitoring tasks 131
roles and rights 116
system administrators
creating accounts 113
deleting 114
disabling 114
editing accounts 114
from LDAP 113
LDAP groups 115, 116
vCenter Single Sign On groups 115
vSphere SSO groups 115
system events 132
system notification settings 121
system settings, email 121
T
Technical Support, to obtain 7
thin provisioning 37, 57, 62
U
updated information 9
upgrade vCenter Server 100
uploading
media 43
vApps 42
user preferences 17
V
vApps
adding vSphere virtual machines 110
backing up 111
force stopping 111
importing from vSphere 111
placing in maintenance mode 111
VCD public console proxy address 128
VCD public REST API base URL 128
VCD public URL 128
vCenter Chargeback 134
vCenter Server, upgrade 100
vCenter Servers
assigning a vShield license 21
attaching 19, 20
confirming settings 20
connecting 20
connection settings 99
disabling 100
reconnecting 100
removing 100
vShield Manager settings 101
vCloud Director overview 11
virtual machines
importing from vSphere 110, 111
migrate 50
virtual servers
add 77
delete 78
edit 78
settings 78
VPN
edit 74
settings 74
VPN tunnel
peer settings 74
remote 74
vShield, licensing 21
vShield for VMware Cloud Director license 21
vShield Manager
connecting 20
settings 101
vSphere
datastores 102
importing media files from 44
importing virtual machines from 43
resources 99
stranded items 103
vSphere distributed switches, setting the MTU 25
vSphere lookup service 129
vSphere VXL AN 48
VXL AN 25, 48
W
web addresses 127
Web console, logging in 13