Cloud Director Administrator's Guide

Cloud Director 1.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000343-00

vmware®

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

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

Contents

About This Book

The *VMware Cloud Director Administrator's Guide* provides information to the Cloud 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 Cloud Director installation. The information in this book is written for experienced system administrators who are familiar with Linux, Windows, IP networks, and VMware vSphere.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting

Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Getting Started with Cloud Director 1

The first time you log in to the Cloud 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 Cloud Director virtual machines.

This chapter includes the following topics:

Overview of Cloud Director Administration

VMware Cloud 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 Cloud 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

Cloud Director relies on vSphere resources to provide CPU and memory to run virtual machines. In addition, vSphere datastores provide storage for virtual machine files and other files necessary for virtual machine operations. Cloud Director also utilizes vNetwork 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 Cloud 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 networks, and network pools. Before you can add cloud resources to Cloud 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.

Cloud Director Networking

Cloud Director supports three types of networks.

- External networks
- Organization networks
- vApp networks

Some organization 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 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 Networks

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

Only system administrators can create organization networks. System administrators and organization administrators can manage organization 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 network to allow the vApp to communicate with other vApps in the organization and outside of the organization, if the organization 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 Cloud 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. Cloud Director uses network pools to create NAT-routed and internal organization 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 Cloud 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

Cloud 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 Cloud 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 Cloud Director user interface by using a Web browser.

For a list of supported browsers, see the *VMware Cloud 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 Cloud Director server host. For example, **`https://cloud.example.com/cloud`**.

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

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

Preparing the System

The **Home** tab in the Cloud 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

Task	For More Information
Attach a vCenter	"Attach a vCenter Server," on page 15
Create a Provider Virtual Datacenter	"Create a Provider Virtual Datacenter," on page 17
Create an External Network	"Add an External Network," on page 18
Create a Network Pool	"Network Pools," on page 19
Create an Organization	"Create an Organization," on page 24
Allocate Resources to an Organization	"Create an Organization vDC," on page 45
Add a Network to an Organization	"Creating Organization Networks," on page 52
Add a Catalog to an Organization	"Add a Catalog to an Organization," on page 73

Create a Microsoft Sysprep Deployment Package

Before Cloud 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, Cloud Director places some files in the `sysprep` folder on the Cloud Director server host. Do not overwrite these files when you create the Sysprep package.

Prerequisites

Access to the Sysprep binary files for Windows 2000, Windows 2003 (32- and 64-bit), and Windows XP (32- and 64-bit).

Procedure

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

Each operating system requires its own folder.

NOTE Folder names are case-sensitive.

Guest OS	Copy Destination
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32-bit)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64-bit)	*SysprepBinariesDirectory* `/win2k3_64`

Guest OS	Copy Destination
Windows XP (32-bit)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64-bit)	*SysprepBinariesDirectory* `/winxp_64`

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

2 Run the `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory* command.

For example, `/opt/vmware/cloud-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/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/cloud-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

Access to the Sysprep binary files for Windows 2000, Windows 2003 (32- and 64-bit), and Windows XP (32- and 64-bit).

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 Cloud Director server host.

Each operating system requires its own folder.

NOTE Folder names are case-sensitive.

Guest OS	Copy Destination
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32-bit)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64-bit)	*SysprepBinariesDirectory* `/win2k3_64`
Windows XP (32-bit)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64-bit)	*SysprepBinariesDirectory* `/winxp_64`

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

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

For example, `/opt/vmware/cloud-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/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-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.

Set User Preferences

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

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 **OK**.

What to do next

Configure an SMTP server and specify the system notification settings. See "Configure SMTP Settings," on page 84 and "Configure System Notification Settings," on page 85.

Change a System Administrator Password

You can change the password for your system administrator account.

You can change the password of local (non-LDAP) users only.

Procedure

1 Click **Preferences** in the title bar of the Web console.

2 Click the **Change Password** tab.

3 Type your current password and then type your new password twice and click **OK**.

Adding Resources to Cloud Director 2

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

This chapter includes the following topics:

Adding vSphere Resources

Cloud Director relies on vSphere resources to provide CPU and memory to run virtual machines. In addition, vSphere datastores provide storage for virtual machine files and other files necessary for virtual machine operations.

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

Attach a vCenter Server

Attach a vCenter Server to make its resources available for use with Cloud 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 Cloud Director. For more information, see the *VMware Cloud Director Installation and Configuration Guide*.

Procedure

1 Open the Attach New vCenter Wizard on page 16

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

2 Provide vCenter Server Connection and Display Information on page 16

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

3 Connect to vShield Manager on page 16

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

4 Confirm Settings and Attach the vCenter Server on page 16

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

Open the Attach New vCenter Wizard

Open the Attach New vCenter wizard to start the process of attaching a vCenter Server to Cloud 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 Cloud 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 Cloud 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

Cloud Director requires vShield Manager to provide network services. Each vCenter Server you attach to Cloud 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.

Cloud 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 Cloud Director license key in the vCenter Server.

Assign a vShield License Key in vCenter

After you attach a vCenter Server to Cloud Director, you must use the vSphere Client to assign a vShield for VMware Cloud 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 Cloud Director license key you received when you purchased Cloud 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 Cloud Director virtual machines and vApps, and access to storage and network connectivity.

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

For more information about organization virtual datacenters, see "Allocate Resources to an Organization," on page 28.

For more information about organization networks, see "Adding Networks to an Organization," on page 32.

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

Create a provider vDC to register vSphere compute, memory, and storage resources for Cloud 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 VMware HA, you should make sure you are familiar with how VMware HA calculates slot size. For more information about slot sizes and customizing VMware HA behavior, see the *VMware vSphere Availability Guide*.

Prerequisites

Before you can create a provider vDC, you must attach at least one vCenter Server with an available resource pool to Cloud 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 Cloud Director license key.

Procedure

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

2 Click the **New Provider vDC** button.

3 Type a name and optional description and click **Next**.

You can use the name and description fields to indicate the vSphere functionality available to the provider vDC, for example, VMware HA.

4 Select a vCenter Server and resource pool and click **Next**.

If the vCenter Server has no available resource pools, then no resource pools appear in the list.

5 Select one or more datastores, click **Add**, and click **Next**.

Cloud Director does not support the use of read-only datastores with provider vDCs. In most cases, read-only datastores do not appear in the list, but some read-only NFS datastores may appear. Do not add these datastores to your provider vDC.

VMware recommends that you use only shared storage. VMware DRS cannot migrate virtual machines on local storage.

6 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 networks.

For more information about organization networks, see "Understanding Organization Networks," on page 32.

Add an External Network

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

Prerequisites

A vSphere port group is available.

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 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 networks.

A network pool is backed by vSphere network resources such as VLAN IDs, port groups, or Cloud isolated networks. Cloud Director uses network pools to create NAT-routed and internal organization 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 Cloud 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

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

Prerequisites

A range of VLAN IDs and a vNetwork 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 the **Add Network Pool** button.
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 vNetwork 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 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 pre-existing port groups in vSphere.

Prerequisites

An available vSphere vNetwork distributed switch.

Procedure

1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.

2 Click the **Add Network Pool** button.

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 vNetwork 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**.

Cloud Director creates Cloud isolated networks in vSphere as they are needed.

What to do next

You can now create an organization 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 21.

Add a Network Pool That Is Backed by vSphere Port Groups

Add a network pool that is backed by port groups to register vSphere port groups for Cloud Director to use. Unlike other types of network pools, a network pool that is backed by port groups does not require a vNetwork distributed switch.

Caution The port groups must be isolated at the layer 2 level from all other port groups. 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.

This is the only type of network pool that works with Cisco Nexus 1000V virtual switches.

Prerequisites

One or more port groups are available in vSphere. The port groups must be available on each ESX/ESXi host in the cluster.

Procedure

1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.

2 Click the **Add Network Pool** button.

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 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 unit (MTU) Cloud Director uses for a network pool that is backed by Cloud isolated networks. MTU is the maximum amount of data that can be transmitted in one packet before it is split into smaller packets.

When both the virtual machine guest operating system and the underlying physical infrastructure are configured with the standard MTU (1500 bytes), then the VMware network isolation protocol will fragment frames. To avoid frame fragmentation, you should increase the MTU to at least 1524 bytes for both 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.

In the unlikely case that your physical network has an MTU of less than the standard of 1500 bytes, then you should decrease the MTU of the network pool to match the underlying physical network.

Prerequisites

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 **Edit Network Pool**.

3 On the **Network Pool MTU** tab, type the MTU and click **OK**.

Cloud Director modifies the MTU for the network pool and all other network pools that use the same vNetwork distributed switch.

Creating and Provisioning Organizations

3

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

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, Cloud Director stops the vApp.

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

When a storage lease expires, Cloud 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 27.

Users can configure email notification to receive a message before a runtime or storage lease expires. See "Set User Preferences," on page 14 for information about lease expiration preferences.

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 24

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

2 Name the Organization on page 25

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

3 Specify the Organization LDAP Options on page 25

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. LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.

4 Add Local Users to the Organization on page 26

Every organization should have at least one local, non-LDAP, organization administrator account, so that user can log in even if the LDAP service is unavailable.

5 Set the Organization Catalog Publishing Policy on page 26

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 27

Cloud 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 27

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 28

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 Cloud 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. 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 85.

Procedure

1 Select the source for organization users.

Option	Description
Do not use LDAP	Organization administrator creates a local user account for each user in the organization. You cannot create groups if you choose this option.
VCD system LDAP service	Use the Cloud Director system LDAP service as the source for organization users and groups.
Custom LDAP service	Connect the organization to its own private LDAP service.

2 Provide any additional information that your selection requires.

Option	Action
Do not use LDAP	Click **Next**.
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 **Next**. 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 **Next** and enter the custom LDAP settings for the organization.

Add Local Users to the Organization

Every organization should have at least one local, non-LDAP, organization administrator account, so that user can log in even if the LDAP service is unavailable.

Procedure

1 Click **Add**.

2 Type a user name and password.

3 Assign a role to the user.

4 Type the contact information for the user.

5 Specify 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 Cloud Director installation.

Procedure

1 Select a catalog publishing option.

Option	Description
Cannot publish catalogs	The organization administrator cannot publish catalogs for users outside of the organization.
Allow publishing catalogs to all organizations	The organization administrator can publish catalogs for users in all organizations.

2 Click **Next**.

Configure Email Preferences

Cloud 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.

Option	Description
Use the system default SMTP server	The organization uses the system SMTP server.
Set organization SMTP server	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.

2 Select a notification settings option.

Option	Description
Use the system default notification settings	The organization uses the system notification settings.
Set organization notification settings	The organization uses its own notification settings. Type an email address that appears as the sender for organization emails, type text to use as the subject prefix for organization emails, and select the recipients for organization emails.

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

4 Click **Next**.

Configure Organization Lease, Quota, and Limit Settings

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

For more information about leases, see "Understanding Leases," on page 23.

Procedure

1 Select the lease options for vApps and vApp templates.

Leases provide a level of control over an organization's storage and compute resources by specifying the maximum amount of time that vApps can 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.

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 you specify act as the default for all new users added to the organization.

3 Select the limits for resource intensive operations.

Certain Cloud 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 may 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 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 29

Open the Allocate Resources wizard to start the process of creating an organization vDC for an organization.

2 Select a Provider vDC on page 29

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 29

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 30

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

5 Allocate Storage on page 31

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 on page 31

A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization networks.

7 Name the Organization vDC on page 32

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

8 Confirm Settings and Create the Organization vDC on page 32

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.

Option	Description
Allocation Pool	Only a percentage of the resources you allocate are committed to the organization vDC. You can specify the percentage, which allows you to overcommit resources.
Pay-As-You-Go	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.
Reservation Pool	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.

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.

Option	Action
CPU allocation	Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization vDC.
CPU resources guaranteed	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%.
Memory allocation	Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization vDC.
Memory resources guaranteed	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%.
vCPU Speed	Enter the vCPU speed in GHz. Virtual machines running in the organization vDC are assigned this amount of GHz per vCPU.
Maximum number of VMs	Enter the maximum number of virtual machines that can be created in the organization vDC.

2 Click **Next**.

Example 3-1. Configuring an Allocation Model

When you create an organization vDC, Cloud Director creates a vSphere resource pool based on the allocation model settings you specify. See Table 3-1, Table 3-2, and Table 3-3.

Table 3-1. How Allocation Pool Settings Affect Resource Pool Settings

Allocation Pool Setting	Allocation Pool Value	Resource Pool Setting	Resource Pool Value
CPU Allocation	25 GHz	CPU Limit	25 GHz
CPU % Guarantee	10%	CPU Reservation	2.5 GHz

Table 3-1. How Allocation Pool Settings Affect Resource Pool Settings (Continued)

Allocation Pool Setting	Allocation Pool Value	Resource Pool Setting	Resource Pool Value
Memory Allocation	50 GB	Memory Limit	50 GB
Memory % Guarantee	20%	Memory Reservation	10 GB

Table 3-2. How Pay-As-You Go Settings Affect Resource Pool Settings

Pay-As-You-Go Setting	Pay-As-You-Go Value	Resource Pool Setting	Resource Pool Value
CPU % Guarantee	10%	CPU Reservation, CPU Limit	0.00 GHz, Unlimited
Memory % Guarantee	100%	Memory Reservation, Memory Limit	0.00 GB, Unlimited

Resource pools created to support Pay-As-You-Go organization vDCs will always have no reservations or limits. Pay-As-You-Go settings only affect overcommitment. A 100% 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

Reservation Pool Setting	Reservation Pool Value	Resource Pool Setting	Resource Pool Value
CPU Allocation	25 GHz	CPU Reservation, CPU Limit	25 GHz, 25 GHz
Memory Allocation	50 GB	Memory Reservation, Memory Limit	50 GB, 50 GB

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.

Procedure

1 Enter the amount of storage to allocate.

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

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, but commits only as much storage space as the disk needs for its initial operations.

3 Click **Next**.

Select Network Pool

A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization 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 Click **Next**.

Name the Organization vDC

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

Procedure

1 Type a name and optional description.

You can use the name and description fields to indicate the vSphere functionality available to the organization vDC, for example, VMware HA.

2 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 Click **Finish** to accept the settings and create the organization vDC.

When you create an organization vDC, Cloud Director creates a resource pool in vSphere to provide CPU and memory resources.

Adding Networks to an Organization

Add a network to an organization to enable its virtual machines to communicate with each other or to provide access to the Internet. A single organization can have multiple organization networks.

Understanding Organization Networks

An organization network allows virtual machines in the organization to communicate with each other and to access the Internet. Organization networks require an external network, a network pool, or both.

Table 3-4 describes the types of organization network.

Table 3-4. Types of Organization Networks and Their Requirements

Organization Network Type	Description	Requirements
External organization network - direct connection	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. Machines outside of this organization can connect to machines within the organization directly.	External network
External organization network - NAT-routed connection	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.	External network and network pool
Internal organization network	Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network. This network provides an organization with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to machines outside this organization. Machines outside of this organization have no connectivity to machines within the organization.	Network pool

Add an External Direct Organization Network

You can add an external direct organization network that multiple organizations can access and is typically used to connect to the Internet. The organization connects directly to this network.

Prerequisites

An external network.

Procedure

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

2 Right-click the organization name and select **Add Networks**.

3 Select the type of setup and network type.

You can create an external direct organization network using either method.

Option	Network Type
Typical	Select the external network check box and select **direct connection** from the drop-down menu.
Advanced	Select **External organization network - direct connection**.

4 Select an external network and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view external networks that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network and later create an organization vDC that can access the network.

5 Type a name and optional description and click **Next**.

6 Review the settings for the organization network.

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

Add an External NAT-Routed Organization Network

You can add an external NAT-routed organization network that only this organization can access. An external NAT-routed organization network provides NAT connectivity to machines outside this organization for fine-tuned control on what is accessible.

Prerequisites

An external network and a network pool.

Procedure

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

2 Right-click the organization name and select **Add Networks**.

3 Select the type of setup and network type.

You can create an external routed organization network using either method.

Option	Network Type
Typical	Select the external network check box and select **routed connection** from the drop-down menu.
Advanced	Select **External organization network - NAT-routed connection**.

4 Select an external network and network pool and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view external networks and network pools that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network or network pool and later create an organization vDC that can access it.

5 Use the default network settings or type your own and click **Next**.

6 (Optional) Type an external IP address for the network to use for NAT services, click **Add**, and click **Next**.

This setting is only available in advanced setup. You can add more than one external IP address.

7 Type a name and optional description and click **Next**.

8 Review the settings for the organization network.

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

What to do next

If you added external IP addresses, you can specify how they get mapped. See "Configure External IP Mapping for an Organization Network," on page 57.

Add an Internal Organization Network

You can add an internal organization network that only this organization can access. It provides the organization with an internal network to which multiple vApps can connect.

Prerequisites

A network pool.

Procedure

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

2 Right-click the organization name and select **Add Networks**.

3 Select the type of setup and network type.

You can create an external routed organization network using either method.

Option	Network Type
Typical	Select the internal network check box.
Advanced	Select **Internal organization network**.

4 Select a network pool and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view network pools that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network pool and later create an organization vDC that can access it.

5 Use the default network settings or type your own and click **Next**.

6 Type a name and optional description and click **Next**.

7 Review the settings for the organization network.

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

Creating a Published Catalog

4

You can publish a catalog to make a set of vApp templates or media files available to all of the organizations in a Cloud 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 Cloud 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

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 Catalog

Create a catalog to contain uploaded and imported vApp templates and media files. An organization can have multiple catalogs and control access to each catalog individually.

Prerequisites

An organization in which to create a catalog.

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 the **New** button.

5 Type a catalog name and optional description and click **Next**.

6 Click **Next**.

7 Select **Published to 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. Cloud Director supports OVF 1.0 and OFV 1.1.

You can quarantine files that users upload to Cloud Director so that you can process the files (for example, scan them for viruses) before accepting them. See "Quarantine Uploaded Files," on page 95.

Prerequisites

The organization to which you are uploading the OVF package must have a catalog and an organization vDC. The computer from which you are uploading must have 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 the **Upload** button.

5 Click **Choose file**, 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 VMware Tools is installed on the virtual machines in the vApp. VMware Tools is required to support guest customization. See the *VMware Cloud Director User's Guide* for more information.

Import a vApp Template from vSphere

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

Prerequisites

You must be a Cloud 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 the **Import from vSphere** button.

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 or not 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

Make sure that VMware Tools is installed on the virtual machines in the vApp. VMware Tools is required to support guest customization. See the *VMware Cloud Director User's Guide* for more information.

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 Cloud Director so that you can process the files (for example, scan them for viruses) before accepting them. See "Quarantine Uploaded Files," on page 95.

Prerequisites

The computer from which you are uploading must have 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 the **Upload** button.

5 Click **Choose file**, 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 Cloud 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

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

Prerequisites

The organization containing 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**.

5 On the Publishing tab, select **Published to Organizations** and click **OK**.

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

Managing Cloud Resources 5

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

This chapter includes the following topics:

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 its resources. The existing organization vDCs of the provider vDC are not affected.

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

Delete a provider vDC to remove its compute, memory, and storage resources from Cloud Director. The resources remain unaffected in vSphere.

Prerequisites

- If you are deleting the only provider vDC in the installation, you must disable it and delete all of its organization vDCs and organization networks.
- If there are other provider vDCs available and enabled, you must disable the provider vDC, delete all of its organization vDCs, and then reset any organization networks that depend on 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**.

Modify a Provider vDC Name and Description

As your Cloud 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, VMware HA.

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**.

Cloud 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 Cloud 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 Cloud Director environment.

For information about moving running virtual machines from one host to another, see "Move Running Virtual Machines from one ESX/ESXi Host to Another," on page 65.

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**.

Cloud 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

Cloud 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**.

Cloud Director upgrades the host agent. This upgrade affects all provider vDCs that use the host.

Repair a Provider vDC ESX/ESXi Host

If the Cloud 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**.

Cloud Director repairs the host. This operation affects all provider vDCs that use the host.

Enable or Disable a Provider vDC Datastore

When you disable a datastore, you cannot start vApps associated with the datastore or create vApps on the datastore.

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 **Enable** or **Disable**.

Cloud Director enables or disables the datastore for all provider vDCs that use its resources.

Add Storage Capacity to a Provider vDC

You can add storage capacity to a provider vDC by adding one or more datastores.

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 Click the **Add** button.

5 Select a datastore from the list, click **Add**, and click **OK**.

Cloud Director does not support the use of read-only datastores with provider vDCs. In most cases, read-only datastores do not appear in the list, but some read-only NFS datastores may appear. Do not add these datastores to your provider vDC.

VMware recommends that you use only shared storage. VMware DRS cannot migrate virtual machines on local storage.

Cloud Director adds the datastore for the provider vDC to use.

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 Cloud Director when the datastore reaches a specific threshold of available capacity. These warnings alert you to a low disk situation before it becomes a problem.

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 Cloud Director sends an email alert, the message indicates which threshold was crossed.

6 Click **OK**.

Cloud 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 the users that own objects (for example, vApps or media files) in the provider vDC. 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 Users**.

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 45

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 46

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

3 Select a Provider vDC on page 46

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 46

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 47

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

6 Allocate Storage on page 48

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 on page 48

A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization networks.

8 Name the Organization vDC on page 49

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

9 Confirm Settings and Create the Organization vDC on page 49

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 **New vDC** button.

Select an Organization for the Organization vDC

You can create an organization vDC to provide resources to any organization in the Cloud 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.

Option	Description
Allocation Pool	Only a percentage of the resources you allocate are committed to the organization vDC. You can specify the percentage, which allows you to overcommit resources.
Pay-As-You-Go	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.
Reservation Pool	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.

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.

Option	Action
CPU allocation	Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization vDC.
CPU resources guaranteed	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%.
Memory allocation	Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization vDC.
Memory resources guaranteed	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%.
vCPU Speed	Enter the vCPU speed in GHz. Virtual machines running in the organization vDC are assigned this amount of GHz per vCPU.
Maximum number of VMs	Enter the maximum number of virtual machines that can be created in the organization vDC.

2 Click **Next**.

Example 5-1. Configuring an Allocation Model

When you create an organization vDC, Cloud Director creates a vSphere resource pool based on the allocation model settings you specify. See Table 5-1, Table 5-2, and Table 5-3.

Table 5-1. How Allocation Pool Settings Affect Resource Pool Settings

Allocation Pool Setting	Allocation Pool Value	Resource Pool Setting	Resource Pool Value
CPU Allocation	25 GHz	CPU Limit	25 GHz
CPU % Guarantee	10%	CPU Reservation	2.5 GHz

Table 5-1. How Allocation Pool Settings Affect Resource Pool Settings (Continued)

Allocation Pool Setting	Allocation Pool Value	Resource Pool Setting	Resource Pool Value
Memory Allocation	50 GB	Memory Limit	50 GB
Memory % Guarantee	20%	Memory Reservation	10 GB

Table 5-2. How Pay-As-You Go Settings Affect Resource Pool Settings

Pay-As-You-Go Setting	Pay-As-You-Go Value	Resource Pool Setting	Resource Pool Value
CPU % Guarantee	10%	CPU Reservation, CPU Limit	0.00 GHz, Unlimited
Memory % Guarantee	100%	Memory Reservation, Memory Limit	0.00 GB, Unlimited

Resource pools created to support Pay-As-You-Go organization vDCs will always have no reservations or limits. Pay-As-You-Go settings only affect overcommitment. A 100% guarantee means no overcommitment is possible. The lower the percentage, the more overcommitment is possible.

Table 5-3. How Reservation Pool Settings Affect Resource Pool Settings

Reservation Pool Setting	Reservation Pool Value	Resource Pool Setting	Resource Pool Value
CPU Allocation	25 GHz	CPU Reservation, CPU Limit	25 GHz, 25 GHz
Memory Allocation	50 GB	Memory Reservation, Memory Limit	50 GB, 50 GB

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.

Procedure

1 Enter the amount of storage to allocate.

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

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, but commits only as much storage space as the disk needs for its initial operations.

3 Click **Next**.

Select Network Pool

A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization 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 Click **Next**.

Name the Organization vDC

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

Procedure

1 Type a name and optional description.

You can use the name and description fields to indicate the vSphere functionality available to the organization vDC, for example, VMware HA.

2 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 Click **Finish** to accept the settings and create the organization vDC.

When you create an organization vDC, Cloud 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 creation of new vApps that use its resources. The existing vApps for the organization vDC are not affected.

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

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

Before you can delete an organization vDC, you must disable it 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**.

Modify an Organization vDC Name and Description

As your Cloud 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 functionality available to the organization vDC, for example, VMware 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**.

These settings only affect vApps that you start from this point on. vApps that are already running are not affected. The usage information that Cloud Director reports for this organization vDC will 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 for 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 **Storage** tab, enter the new storage settings and 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 On the **Network Pool** tab, enter the new network settings and click **OK**.

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 Cloud 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 Cloud Director.

Prerequisites

Before you can delete an external network, you must delete all of the organization 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 Organization Networks

Only a system administrator can add, reset, and delete an organization network.

System administrators and organization administrators can modify organization network properties, configure organization network services, and view IP address allocations.

Creating Organization Networks

Add a network to an organization to enable its virtual machines to communicate with each other or to provide access to the Internet. A single organization can have multiple organization networks.

Table 5-4 describes the types of organization network.

Table 5-4. Types of Organization Networks and Their Requirements

Organization Network Type	Description	Requirements
External organization network - direct connection	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. Machines outside of this organization can connect to machines within the organization directly.	External network
External organization network - NAT-routed connection	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.	External network and network pool
Internal organization network	Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network. This network provides an organization with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to machines outside this organization. Machines outside of this organization have no connectivity to machines within the organization.	Network pool

Create an External Direct Organization Network

You can create an external direct organization network that multiple organizations can access and is typically used to connect to the Internet. The organization connects directly to this network.

Prerequisites

An external network.

Procedure

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

2 Click the **Add Network** button.

The Create Organization Network wizard starts.

3 Select an organization and click **Next**.

4 Select the type of setup and network type.

You can create an external direct organization network using either method.

Option	Network Type
Typical	Select the external network check box and select **direct connection** from the drop-down menu.
Advanced	Select **External organization network - direct connection**.

5 Select an external network and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view external networks that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network and later create an organization vDC that can access the network.

6 Type a name and optional description and click **Next**.

7 Review the settings for the organization network.

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

Create an External NAT-Routed Organization Network

You can create an external NAT-routed organization network that only this organization can access. An external NAT-routed organization network provides NAT connectivity to machines outside this organization for fine-tuned control on what is accessible.

Prerequisites

An external network and a network pool.

Procedure

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

2 Click the **Add Network** button.

The Create Organization Network wizard starts.

3 Select an organization and click **Next**.

4 Select the type of setup and network type.

You can create an external routed organization network using either method.

Option	Network Type
Typical	Select the external network check box and select **routed connection** from the drop-down menu.
Advanced	Select **External organization network - NAT-routed connection**.

5 Select an external network and network pool and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view external networks and network pools that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network or network pool and later create an organization vDC that can access it.

6 Use the default network settings or type your own and click **Next**.

7 (Optional) Type an external IP address for the network to use for NAT services, click **Add**, and click **Next**.

This setting is only available in advanced setup. You can add more than one external IP address.

8 Type a name and optional description and click **Next**.

9 Review the settings for the organization network.

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

What to do next

If you added external IP addresses, you can specify how they get mapped. See "Configure External IP Mapping for an Organization Network," on page 57.

Create an Internal Organization Network

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

Prerequisites

A network pool.

Procedure

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

2 Click the **Add Network** button.

The Create Organization Network wizard starts.

3 Select an organization and click **Next**.

4 Select the type of setup and network type.

You can create an external routed organization network using either method.

Option	Network Type
Typical	Select the internal network check box.
Advanced	Select **Internal organization network**.

5 Select a network pool and click **Next**.

You can deselect the **Only use networks accessible by this organization** check box to view network pools that are not currently available to the organization through its organization vDCs. This enables you to choose an arbitrary network pool and later create an organization vDC that can access it.

6 Use the default network settings or type your own and click **Next**.

7 Type a name and optional description and click **Next**.

8 Review the settings for the organization network.

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

Configuring Network Services

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

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

Table 5-5. Network Services Available by Network Type

Network Type	DHCP	Firewall	NAT
External organization network - direct connection			
External organization network - NAT-routed connection	X	X	X
Internal organization network	X		

Configure DHCP for an Organization Network

You can configure certain organization networks to provide DHCP services to virtual machines in the organization.

When you enable DHCP for an organization network, connect a NIC on virtual machine in the organization to that network, and select **DHCP** as the IP mode for that NIC, Cloud Director assigns a DHCP IP address to the virtual machine when you power it on.

Both system administrators and organization administrators can configure DHCP.

Prerequisites

An external NAT-routed organization network or an internal organization network.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

3 Click the **DHCP** tab and select **Enable DHCP**.

4 Type a range of IP addresses or use the default range.

Cloud Director uses these addresses to satisfy DHCP requests. The range of DHCP IP addresses cannot overlap with the static IP pool for the organization network.

5 Set the default lease time and maximum lease time or use the default values.

6 Click **OK**.

Cloud Director updates the network to provide DHCP services.

Enable the Firewall for an Organization Network

You can configure certain organization networks to provide firewall services. Enable the firewall on an organization network to block all incoming traffic.

You can also add firewall rules to allow traffic that matches the rules to pass through the firewall. See "Add a Firewall Rule for an Organization Network," on page 56.

Both system administrators and organization administrators can enable firewalls.

Prerequisites

An external NAT-routed organization network.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

3 Click the **Firewall** tab and select **Enable firewall**.

Add a Firewall Rule for an Organization Network

You can add firewall rules to an organization network that supports a firewall to allow traffic that matches the rules to pass through the firewall.

In order for a firewall rule to be enforced, you must enable the firewall for the organization network. See "Enable the Firewall for an Organization Network," on page 55.

Both system administrators and organization administrators can add firewall rules.

Prerequisites

An external NAT-routed organization network.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

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

4 Type a name for the rule.

5 Type the IP address of the virtual machine for which you want to allow incoming traffic.

6 Select the port for incoming traffic.

7 Select the protocol of the incoming traffic to accept.

8 Select the **Enable** check box and click **OK**.

Enable IP Masquerading for an Organization Network

You can configure certain organization networks to provide IP masquerade services. Enable IP masquerading on an organization network to hide the internal IP addresses of virtual machines from the external network.

When you enable IP masquerade, Cloud Director translates a virtual machine's private, internal IP address into a public IP address for outbound traffic.

Both system administrators and organization administrators can enable IP masquerade.

Prerequisites

An external NAT-routed organization network.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

3 Click the **NAT - External IP Mapping** tab and select **Enable IP Masquerade**.

Add External IP Addresses to an Organization Network

Before you can configure external IP mapping for an organization network, you must add one or more external IP addresses.

Only a system administrator can add external IP addresses to an organization network.

Prerequisites

An external NAT-routed organization network.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

3 Click the **NAT - External IPs** tab.

4 Type an IP address and click **Add**.

The IP address must be routable on the external network and unique across internal networks.

5 Click **OK**.

What to do next

Configure external IP mapping using the external IP address.

Configure External IP Mapping for an Organization Network

You can configure certain organization networks to provide external IP mapping. External IP mapping provides external access to services running on virtual machines on the organization network.

When you configure external IP mapping, Cloud Director maps an external IP address and a port to a service running on a port on a virtual machine for inbound traffic.

Both system administrators and organization administrators can configure external IP mapping.

Prerequisites

An external NAT-routed organization network and an external IP address.

Procedure

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

2 Right-click the organization network name and select **Configure Services**.

3 Click the **NAT- External IP Mapping** tab and click **Add**.

4 Configure the port forwarding rule.

a Select an external IP address.

b Select an external port.

c Type the IP address of the destination virtual machine.

- If the virtual machine is fenced, type its external IP address.
- If the virtual machine is not fenced, type its internal IP address.

d Select an internal port.

e Select a protocol for the type of traffic to forward.

f Click **OK**.

5 Click **OK**.

Reset an Organization Network

If the network services, such as DHCP settings, firewall settings, and so on, that are associated with an organization network are not working as expected, reset the network.

Before you delete a provider vDC, you should reset the organization networks that depend on it.

No network services are available while an organization network resets.

Prerequisites

An external NAT-routed organization network or an internal organization network.

Procedure

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

2 Right-click the organization network name and select **Reset Network**.

3 Click **Yes**.

Delete an Organization Network

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

Prerequisites

Verify that no virtual machines are connected to the organization network.

Procedure

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

2 Right-click the organization network name and select **Delete Network**.

View IP Usage for an Organization Network

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

Procedure

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

2 Right-click the organization network name and select **IP Allocations**.

Add IP Addresses to an Organization Network IP Pool

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

Prerequisites

An external NAT-routed organization network or an internal organization network.

Procedure

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

2 Right-click the organization 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**.

Modify an Organization Network Name and Description

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

Procedure

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

2 Right-click the organization network name and select **Properties**.

3 On the **Name and Description** tab, type a new name and optional description and click **OK**.

Modify an Organization Network DNS Settings

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

Prerequisites

An external NAT-routed organization network or an internal organization network.

Procedure

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

2 Right-click the organization network name and select **Properties**.

3 On 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 Cloud 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 **Edit Network Pool**.

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

- A network pool that is backed by a port group
- 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 **Edit Network Pool**.

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 **Edit Network Pool**.

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

- 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 **Edit Network Pool**.

3 On the **Network Pool Settings** tab, type a VLAN ID range and click **Add**.

4 Select a vNetwork distributed switch and click **OK**.

Delete a Network Pool

Delete a network pool to remove it from Cloud Director.

Prerequisites

- The network pool is not associated with any organization vDC.
- The network pool is not in use by any vApps.
- The network pool is not used by any NAT-routed or internal organization networks.

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 Network Pool**.

Managing Cloud Cells

You manage cloud cells mostly from the Cloud Director server host on which the cell resides, but you can delete a cloud cell from the Cloud Director Web console.

Table 5-6 lists the basic commands for controlling a cloud cell.

Table 5-6. Cloud Cell Commands

Command	Description
`service vmware-vcd start`	Starts the cell
`service vmware-vcd restart`	Restarts the cell
`service vmware-vcd stop`	Stops the cell

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 61.

Adding Cloud Cells

To add cloud cells to a Cloud Director installation, install the Cloud Director software on additional Cloud Director server hosts in the same Cloud Director cluster.

For more information, see the *VMware Cloud Director Installation and Configuration Guide*.

Delete a Cloud Cell

If you want to remove a cloud cell from your Cloud 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**.

Cloud 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 that attempt to log in to the cell from browser will see a message stating that the cell is down for maintenance. Uses that attempt to reach the cell using the vCloud API will receive a similar message.

Procedure

1 Stop the cell using the `service vmware-vcd stop` command.

2 Run the `/opt/vmware/cloud-director/bin/vmware-vcd-cell maintenance` command.

Users cannot access the cell using a browser or the vCloud API.

Turn Off Cloud Cell Maintenance Message

When you are finished performing maintenance on a cell and ready to restart the cell, you can turn off the maintenance message.

Procedure

1 Run the `/opt/vmware/cloud-director/bin/vmware-vcd-cell stop` command.

2 Start the cell using the `service vmware-vcd start` command.

Users can now access the cell using a browser or the vCloud API.

Managing vSphere Resources 6

After you add vSphere resources to the Cloud Director system, you can perform some management functions from Cloud 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

After you attach a vCenter Server to Cloud Director, you can modify its settings, reconnect to the vCenter Server, and enable or disable it.

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 Cloud 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 Cloud 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 vCenter** or **Enable vCenter**.

3 Click **Yes**.

Remove a vCenter Server

You can remove a vCenter Server to stop using its resources with Cloud 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 vCenter**.

3 Click **Yes**.

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 Cloud 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**.

Cloud Director enables or disables the host for all provider vDCs that use its resources.

Move Running Virtual Machines from one ESX/ESXi Host to Another

You can move all the virtual machines that are running on one ESX/ESXi host to another. This is useful if you want to unprepare a host, or if you want to perform maintenance on a host without affecting running virtual machines.

Prerequisites

You must 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**.

Cloud Director puts the host into maintenance mode and moves all its running virtual machines to another host in the same cluster.

Prepare or Unprepare an ESX/ESXi Host

When you add an ESX/ESXi host to a vSphere cluster that Cloud 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 Cloud Director environment.

For information about moving running virtual machines from one host to another, see "Move Running Virtual Machines from one ESX/ESXi Host to Another," on page 65.

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 **Hosts** in the left pane.

2 Right-click the host name and select **Prepare Host** or **Unprepare Host**.

If you are preparing a host, type a user name and password and click **OK**.

Cloud Director prepares or unprepares the host for all provider vDCs that use its resources.

Upgrade an ESX/ESXi Host Agent

Cloud 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 Cloud 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 Cloud Director system and also configure low disk space warnings for each datastore.

Enable or Disable a Datastore

When you disable a datastore, you cannot start vApps 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**.

Cloud Director enables or disables the datastore for all provider vDCs that use its resources.

Configure Low Disk Space Warnings for a Datastore

You can configure low disk space warnings on a datastore to receive an email from Cloud Director when the datastore reaches a specific threshold of available capacity. These warnings alert you to a low disk situation before it becomes a problem.

Procedure

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

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

3 Select the disk space thresholds for the datastore.

You can set two thresholds, yellow and red. When Cloud Director sends an email alert, the message indicates which threshold was crossed.

4 Click **OK**.

Cloud Director sends an email alert when the datastore crosses a threshold.

Managing Stranded Items

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

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

Delete a Stranded Item

You can delete a stranded item to attempt to remove an object from vSphere that you already deleted from Cloud 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**.

Cloud Director attempts to delete the stranded item from vSphere.

3 Refresh the page display.

If the delete operation is successful, Cloud 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 67.

Force Delete a Stranded Item

If Cloud Director is unable to delete a stranded item, you can force delete it to remove it from the stranded items list. The stranded item will continue to exist in vSphere.

Before you force delete a stranded item, try to delete it. See "Delete a Stranded Item," on page 67.

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**.

Cloud Director removes the item from the stranded items list.

Managing Organizations 7

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

Disabling an organization prevents users from logging in to the organization. Currently logged in users are not affected and 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 Cloud 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**.

Modify an Organization Name

As your Cloud 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 Cloud 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 85.

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.

Option	Description
Do not use LDAP	Organization administrator creates a local user account for each user in the organization. You cannot create groups if you select this option.
VCD system LDAP service	Use the LDAP service for the Cloud Director system as the source for organization users and groups.
Custom LDAP service	Connect the organization to its own private LDAP service.

5 Provide any additional information required by your selection.

Option	Action
Do not use LDAP	Click **OK**.
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 Cloud 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**.

Option	Description
Cannot publish catalogs	Organization administrator cannot publish any catalogs for users outside of the organization.
Allow publishing catalogs to all organizations	Organization administrator can publish a catalog for users in all organizations.

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

Cloud 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.

Option	Description
Use system default SMTP server	Organization uses the system SMTP server.
Set organization SMTP server	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.

5 Select a notification settings option.

Option	Description
Use system default notification settings	Organization uses the system notification settings.
Set organization notification settings	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.

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

7 Click **OK**.

Modify Organization Lease, Quota, and Limit Settings

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

For more information about leases, see "Understanding Leases," on page 23.

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.

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.

5 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 quota you specify affects all the users in the organization.

6 Select the limits for resource intensive operations.

Certain Cloud 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.

7 Select the number of simultaneous connections for each virtual machine and click **OK**.

Add a Catalog to an Organization

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

An organization in which to create a catalog.

Procedure

1 Click the **Home** tab and click **Add another 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 click **Next**.

Option	Description
Do not publish this catalog to other organizations	The items added to the catalog are only available within the organization.
Published to Organizations	The items added to the catalog are available to all of the organizations in the Cloud Director installation. The administrators of each organization can then choose which catalog items to provide to their users.

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

Managing Organization Resources

Cloud 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 45.

For information about removing an organization vDC, see "Delete an Organization vDC," on page 49.

For information about modifying the resources available to an existing organization vDC, see "Edit Organization vDC Allocation Model Settings," on page 50, and "Edit Organization vDC Storage Settings," on page 50.

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 Cloud Director User's Guide*.

Managing Organization vApps

There are a couple of tasks related to managing organization vApps that can only be performed by a system administrator. System administrators can import a vApp from vSphere and can force stop a running vApp.

For more information about working with vApps in an organization, see the *VMware Cloud Director User's Guide*.

Import a vSphere Virtual Machine as a vApp

A system administrator can import a vSphere virtual machine as a Cloud Director vApp.

Prerequisites

You must be logged in to Cloud 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 Click the **Import from vSphere** button.

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**.

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 Cloud 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 Cloud 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**.

Managing System Administrators and Roles

8

You can add system administrators to Cloud Director individually, or as part of an LDAP group. You can also add and modify the roles that determine what rights a user has within their organization.

This chapter includes the following topics:

Add a System Administrator

You can add a system administrator to Cloud Director by creating a new system administrator account. System administrators have full rights to Cloud Director and all of its organizations.

Procedure

1 Click the **Administration** tab and click **Users** in the left pane.

2 Click the **Add User** button.

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 as a system administrator. System administrators have full rights to Cloud Director and all of its organizations.

Prerequisites

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

Procedure

1 Click the **Administration** tab and then click **Users** in the left pane.

2 Click the **Import User** button.

3 Type a full or partial name in the text box and click **Search Users**.

4 Select the users to import and click **Add**.

5 Click **OK**.

Enable or Disable a System Administrator

You can disable a system administrator user to prevent that user from logging in to Cloud 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** or **Disable**.

Delete a System Administrator

You can remove a system administrator from the Cloud 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 User**.

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 non-LDAP 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 the users in the entire installation, all system administrators, or all organization administrators. 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 **Administration** tab and click **Users** in the left pane.

2 Click the **Notify Users** button.

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 Cloud 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 77 and "Import a System Administrator," on page 78.

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 an LDAP Group

To add a group of users with system administrator rights, you can import an LDAP group as system administrators. System administrators have full rights to Cloud Director and all of its organizations.

Prerequisites

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

Procedure

1 Click the **Administration** tab and click **Groups** in the left pane.

2 Click the **Import Group** button.

3 Type a full or partial name in the text box and click **Search Groups**.

4 Select the groups to import and click **Add**.

5 Click **OK**.

Delete an LDAP Group

You can remove a group of system administrators from the Cloud Director system by deleting their LDAP group.

When you delete an LDAP group, users who have a Cloud Director account based solely on their membership in that group will become stranded and unable to log in. See "Delete a System Administrator Who Lost Access to the System," on page 79.

Procedure

1 Click the **Administration** tab and click **Groups** in the left pane.

2 Right-click the group name and select **Delete Group**.

3 Click **Yes** to confirm the deletion.

Change an LDAP Group Description

You can add or modify the description of an LDAP group to provide more information about the group.

Procedure

1 Click the **Administration** tab and click **Groups** in the left pane.

2 Right-click the group name and select **Properties**.

3 Type a description for the group and click **OK**.

Roles and Rights

Cloud Director uses roles and rights to determine what actions a user can perform in an organization. Cloud 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 97.

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 the **New Role** button.

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 if you no longer need it. 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 Role**.

3 Click **Yes** to confirm the deletion.

Managing System Settings 9

A Cloud 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

Cloud 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 83.

Procedure

1 Click the **Administration** tab and click **General** in the left pane.

2 Modify the settings and click **Apply**.

General System Settings

Cloud Director includes a number of general system settings that you can modify to meet your needs.

Table 9-1 describes each of the general system settings.

Table 9-1. General System Settings

Name	Category	Description
Synchronization Start Time	LDAP Synchronization	Time of day to start LDAP synchronization.
Synchronization Interval	LDAP Synchronization	The number of hours between LDAP synchronizations.

Table 9-1. General System Settings (Continued)

Name	Category	Description
Login Policy	Login Policy	Select a login policy.
Activity Log History to keep	Activity Log	Number of days of log history to keep before deleting it. Type **0** to never delete logs.
Activity Log History shown	Activity Log	Number of days of log history to display. Type **0** to show all activity.
Display debug information	Activity Log	Enable this setting to display debug information in the Cloud Director task log.
Idle Session Timeout	Miscellaneous	Amount of time the Cloud Director application remains active without user interaction.
Maximum Session Timeout	Miscellaneous	Maximum amount of time the Cloud Director application remains active.
Host Refresh Frequency	Miscellaneous	How often Cloud Director checks whether its ESX/ESXi hosts are accessible or inaccessible.
Host Hung Timeout	Miscellaneous	Select the amount of time to wait before marking a host as hung.
Chargeback Event History to Keep	Miscellaneous	Number of days of chargeback event history to keep before deleting it.
Provide default vApp names	Miscellaneous	Select the check box to generate default names for vApps.
Allow Overlapping External Networks	Miscellaneous	Select the check box if you want to add external networks that run on the same network segment. You should only enable this setting if you are using non-VLAN-based methods (for example, VMware vShield Manager) to isolate your external networks.
Enable Upload Quarantine with a Timeout of __ seconds	Miscellaneous	Select the check box and enter a timeout representing the amount of time to quarantine uploaded files. For more information about working with quarantined files, see "Monitoring Quarantined Files," on page 94.
Verify vCenter certificates	Miscellaneous	Select the check box to only allow Cloud Director to communicate with trusted vCenter servers. Click **Browse** to locate the JCEKS keystore and type the keystore password.

Configure SMTP Settings

Cloud 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 Cloud Director emails.

Cloud 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 Cloud 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

Cloud Director sends system alert emails when it has important information to report. For example, Cloud Director sends an alert when a datastore is running out of space. You can configure Cloud Director to send email alerts to all system administrators or to a specified list of email addresses.

Organizations can use the system notification settings, or use custom notification settings.

Prerequisites

A valid connection to an SMTP server.

Procedure

1 Click the **Administration** tab and click **Email** in the left pane.

2 Select the recipients of system alert emails and click **Apply**.

Configuring the System LDAP Settings

You can configure Cloud 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 Cloud 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 Cloud Director until you import them to the system or an organization.

When an imported LDAP user logs in to Cloud Director, Cloud Director checks the credentials of the user against the LDAP directory. If the credentials are accepted, Cloud Director creates a user account and logs the user in to the system.

Cloud 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 Cloud Director synchronizes user and group information with the LDAP directory.

LDAP Support

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

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

Table 9-2. Supported Combinations of Operating System, LDAP Server, and Authentication Method

Operating System	LDAP Server	Authentication Method
Windows 2003	Active Directory	Simple
Windows 2003	Active Directory	Simple SSL
Windows 2003	Active Directory	Kerberos
Windows 2003	Active Directory	Kerberos SSL
Windows 2008	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple SSL
Windows 7 (2008 R2)	Active Directory	Kerberos

Table 9-2. Supported Combinations of Operating System, LDAP Server, and Authentication Method (Continued)

Operating System	LDAP Server	Authentication Method
Windows 7 (2008 R2)	Active Directory	Kerberos SSL
Linux	OpenLDAP	Simple
Linux	OpenLDAP	Simple SSL

Configure an LDAP Connection

You can configure an LDAP connection to provide Cloud 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 87.

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 Cloud 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 Cloud Director.

5 Select the SSL check box to use LDAPS and choose one of the certificate options.

Option	Action
Accept all certificates	Select the check box.
SSL Certificate	Click **Browse** to locate the SSL certificate.
SSL Keystore	Click **Browse** to locate the SSL keystore. Type and confirm the keystore password.

6 Select an authentication method.

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

7 Type a user name and password to connect to the LDAP server.

If anonymous read support is enabled on your LDAP server, you can leave these text boxes blank.

Authentication Method	User Name Description
Simple	Type the full LDAP DN.
Kerberos	Type the name in the form of *user@REALM.com*.

8 Click **Apply**.

What to do next

You can now add LDAP users and groups to the system and to organizations that use the system LDAP settings.

Add a Kerberos Realm

Cloud 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 On the **Realm** tab, click **Add**.

4 Type a realm and its Key Distribution Center (KDC) and click **OK**.

The realm name must be all capital letters. For example, `REALM`.

5 On the **DNS** tab, click **Add**.

6 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`.

7 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 Cloud Director with details about how user and group information is defined in the LDAP directory. Cloud 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 Cloud Director with the LDAP Server

Cloud 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 83.

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 Cloud Director Client UI

You can customize the branding of the Cloud Director client UI and some of the links that appear on the Cloud Director Home login screen.

For a sample .css template with information about the styles that Cloud Director supports for custom themes, see http://kb.vmware.com/kb/1026050.

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**.

The logo appears in the title bar for all users. The file must be 48-by-48 pixels and in the PNG, JPEG, or GIF format.

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 Cloud 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 Cloud Director installation.

   The **Support** link on the **Home** tab of all Cloud Director organizations will open this URL.

7 Type a URL that links to a web site that allows users to sign up for a Cloud Director account.

   This link appears on the Cloud 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 Cloud Director login page.

9 Click **Apply**.

Configure the Public Web URL

If your Cloud 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, Cloud 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. Cloud Director also modifies the organization URLs of existing organizations.

Configure the Public Console Proxy Address

If your Cloud 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, Cloud 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 Cloud 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, Cloud 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.

Monitoring Cloud Director 10

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

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

Cloud 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`.

Cloud Director events represent one-time occurrences that typically indicate an important part of an operation or a significant state change for a Cloud Director object. For example, Cloud Director logs an event when a user initiates the creation an organization vDC and another event when the process completes. Cloud 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 92.

The log can also include debug information, depending on your Cloud Director settings. See "General System Settings," on page 83.

Procedure

1 Log in to the Cloud Director system as a system administrator.

2 Click the **Manage & Monitor** tab and click **Logs** in the left pane.

3 Click the **Tasks** tab.

Cloud 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 91.

The log can also include debug information, depending on your Cloud Director settings. See "General System Settings," on page 83.

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.

Cloud 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 92.

Procedure

1 Log in to the Cloud Director system as a system administrator.

2 Click the **Manage & Monitor** tab and click **Logs** in the left pane.

3 Click the **Events** tab.

Cloud Director displays information about each system-level event.

4 Double-click an event for more information.

View Organization Events

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 92.

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.

Cloud Director displays information about each organization-level event.

5 Double-click an event for more information.

Only system administrators can view the details about most events.

View Usage Information for a Provider vDC

Provider vDCs supply compute, memory, and storage resources to organization vDCs. 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.

Cloud Director displays information about available 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. 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.

Cloud Director displays information about available CPU, memory, and storage for each organization vDC.

Using Cloud Director's JMX Service

Each Cloud 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 Cloud Director JMX service. JConsole is an example of a JMX client.

For more information about the MBeans exposed by Cloud Director, see http://kb.vmware.com/kb/1026065.

Prerequisites

The host name of the Cloud 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 Cloud Director server, followed by the port number. For example, **`example.com:8999`**. The default port is 8999.

4 Type a Cloud Director system administrator user name and password and click **Connect**.

5 Click the **MBeans** tab.

Viewing the Cloud Director Logs

Cloud 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/cloud-director/logs`. Table 10-1 lists the available logs.

Table 10-1. Cloud Director Logs

Log Name	Description
cell.log	Console output from the Cloud Director cell.
vcloud-container-debug.log	Debug-level log messages from the cell.
vcloud-container-info.log	Informational log messages from the cell. This log also shows warnings or errors encountered by the cell.
vmware-vcd-watchdog.log	Informational log messages from the cell watchdog. It records when the cell crashes, is restarted, and so on
diagnostics.log	Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.
YYYY_MM_DD.request.log	HTTP request logs in the Apache common log format.

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

Cloud Director and Cost Reporting

You can use VMware vCenter Chargeback 1.5 to configure a cost reporting system for VMware Cloud Director.

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

You can specify the number of days of chargeback history that Cloud Director saves. See "Modify General System Settings," on page 83.

Monitoring Quarantined Files

Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud Director server, followed by the port number. For example, **`example.com:8999`**. The default port is 8999.

4 Type a Cloud 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.

7 Copy the text of the message to which you want to respond.

For example,

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<QuarantineRequestMessage transferSessionId="239d310a-5bce-492d-9e26-eda6b646dc15"
transferSessionFilePath="/opt/vmware/cloud-director/data/transfer/239d310a-5bce-492d-9e26-
eda6b646dc15"
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 version="1.0" encoding="UTF-8" standalone="yes"?>
<QuarantineResponseMessage transferSessionId="239d310a-5bce-492d-9e26-eda6b646dc15"
transferSessionFilePath="/opt/vmware/cloud-director/data/transfer/239d310a-5bce-492d-9e26-
eda6b646dc15"
response="accept"
xmlns="http://www.vmware.com/vcloud/v1"/>
```

3 Start JConsole.

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 Cloud Director server, followed by the port number. For example, **`example.com:8999`**. The default port is 8999.

6 Type a Cloud 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 Cloud Director system administrator user name and password in the other fields.

10 Click **sendTextMessage**.

For an accepted file, Cloud Director releases the file from quarantine and completes the upload. For a rejected file, Cloud Director removes the file.

11 Roles and Rights

Cloud 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.

Cloud Director includes several predefined roles.

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

Predefined Roles and Their Rights

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

Table 11-1 lists the predefined Cloud Director roles and the default rights assigned to each role. 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

	System Administrator	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
vApp: Create a vApp	X	X	X	X		
vApp: Delete a vApp	X	X	X	X	X	
vApp: Edit vApp Properties	X	X	X	X	X	
vApp: Start/Stop/ Suspend/Reset a vApp	X	X	X	X	X	
vApp: Share a vApp	X	X	X	X	X	
vApp: Copy/ Move a vApp	X	X	X	X	X	
vApp: Access to VM Console	X	X	X	X	X	X

Table 11-1. Default Rights for the Predefined Roles (Continued)

	System Administrator	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
vApp: Change Owner	X	X				
vApp: Edit VM Properties	X	X	X	X	X	
vApp: Edit VM Memory	X	X	X	X		
vApp: Edit VM CPU	X	X	X	X		
vApp: Edit VM Network	X	X	X	X		
vApp: Edit VM Hard Disk	X	X	X	X		
vApp: Manage VM Password Settings	X	X	X	X	X	X
Catalog: Create/ Delete a new Catalog	X	X	X			
Catalog: Edit Catalog Properties	X	X	X			
Catalog: Add a vApp from My Cloud	X	X	X	X		
Catalog: Publish a Catalog	X	X	X			
Catalog: Share a Catalog	X	X	X			
Catalog: View Private and Shared Catalogs	X	X	X	X		
Catalog: View Published Catalogs	X	X				
Catalog: Change Owner	X	X				
Catalog Item: Edit vApp Template/Media Properties	X	X	X			
Catalog Item: Create/Delete/ Upload a vApp Template or Media	X	X	X			
Catalog Item: Download a vApp Template	X	X	X			

Table 11-1. Default Rights for the Predefined Roles (Continued)

	System Administrator	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
Catalog Item: Copy/Move a vApp Template or Media	X	X	X	X		
Catalog Item: View vApp Templates and Media	X	X	X	X	X	
Catalog Item: Add to My Cloud	X	X	X	X	X	
Organization: Edit Organization Properties	X	X				
Organization: Edit SMTP Settings	X	X				
Organization: Edit Quotas Policy	X	X				
Organization: View Organizations	X	X				
Organization: Edit Organization Network Properties	X	X				
Organization: View Organization Networks	X	X				
Organization: Edit Leases Policy	X	X				
Organization vDC: View Organization vDCs	X	X				
User: Create/ Import/Delete Group or User	X	X				
User: Edit Group or User Properties	X	X				
User: View Group or User	X	X				
General: Send Notification	X	X				

Table 11-1. Default Rights for the Predefined Roles (Continued)

	System Administrator	Organization Administrator	Catalog Author	vApp Author	vApp User	Console Access Only
General: Administrator Control	X	X				
General: Administrator View	X	X				

Index